DETERMINAN PERILAKU PENGHINDARAN KEJAHATAN SIBER KEUANGAN OLEH PEKERJA SEKTOR KEUANGAN DI INDONESIA

TESIS

Oleh:

Nama : Hanifah Zahra
NIM : 21919012

PROGRAM STUDI MAGISTER AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

2023

DETERMINAN PERILAKU PENGHINDARAN KEJAHATAN SIBER KEUANGAN OLEH PEKERJA SEKTOR KEUANGAN DI INDONESIA

TESIS

Disusun dan diajukan untuk memenuhi salah satu syarat untuk mencapai derajat Magister Strata-2 Program Studi Magister Akuntansi pada Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia

Oleh:

Nama: Hanifah Zahra

No. Mahasiswa: 21919012

PROGRAM STUDI MAGISTER AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

2023

BERITA ACARA UJIAN TESIS

Pada hari Selasa tanggal 25 Juli 2023 Program Studi Akuntansi Program Magister, Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia telah mengadakan ujian tesis yang disusun oleh :

HANIFAH ZAHRA

No. Mhs. : 21919012

Konsentrasi : Audit Forensik

Dengan Judul:

DETERMINAN PERILAKU PENGHINDARAN KEJAHATAN SIBER KEUANGAN OLEH PEKERJA SEKTOR KEUANGAN DI INDONESIA

Berdasarkan penilaian yang diberikan oleh Tim Penguji,

maka tesis tersebut dinyatakan **LULUS**

Penguji I	Penguji II
Drs. Dekar Urumsah,S.Si.,M.Com.,Ph.D.,CFrA.	Prof. Dr. Hadri Kusuma, M.B.A.

Mengetahui

Ketua Program Studi,

Arief Rahman, S.E., S.I.P., M.Com., Ph.D.

PERNYATAAN BEBAS PLAGIARISME

"Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar magister di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam referensi. Apabila dikemudian hari terbukti bahwa pernyataan ini tidak benar maka saya sanggup menerima hukuman/sanksi sesuai dengan peraturan yang berlaku."

Yogyakarta, 21 Juli 2023

Penulis

(Hanifah Zahra)

HALAMAN PENGESAHAN

Yogyakarta, 21 Juli 2023

Telah diterima dan disetujui dengan baik oleh :

Dosen Pembimbing

Drs. Dekar Urumsah,S.Si.,M.Com.,Ph.D.,CFrA.

KATA PENGANTAR

Bismillahirrahmanirrahim,

Asslamualaikum Warahmatullahi Wabarakatuhu,

Puji syukur kehadirat Allah SWT atas segala rahmat dan hidayah-Nya serta segala kemudahan dan kelancaran sehingga penulis dapat menyelesaikan penelitian dengan judul "Determinan Perilaku Penghindaran Kejahatan Siber Keuangan oleh Pekerja Sektor Keuangan di Indonesia". Sholawat serta salam semoga selalu tercurah kepada Rasulullah SAW. Penyusunan penelitian ini disusun guna memenuhi salah satu syarat untuk memperoleh gelar Magister Akuntansi di Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia.

Penulis menyadari bahwa dalam penulisan penelitian ini masih terdapat kekurangan, oleh karena itu penulis mengharapkan kritik dan saran yang membangun demi perbaikan oleh penelitian-penelitian berikutnya.

Keberhasilan penulis dalam menyelesaikan penelitian ini tidak terlepas dari bimbingan, arahan, dan dukungan dari berbagai pihak yang telah memberikan bantuan kepada penulis. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberi rahmat dan ridho yang tiada henti sehingga penulis dapat menyelesaikan karya tulis ini dengan baik.
2. Nabi Muhammad SAW, sebagai panutan umat muslim yang penuh dengan kemuliaan dan ketaatan kepada Allah SWT.

3. Kedua orangtua penulis yang telah membesarkan penulis dengan penuh kasih sayang, serta senantiasa memberikan nasihat, bimbingan, dukungan, dan doa yang tidak pernah berhenti diberikan untuk penulis.
4. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D selaku Rektor Universitas Islam Indonesia.
5. Bapak Johan Arifin, S.E., M.Si., Ph.D., CFrA., Cert.IPSAS selaku Dekan Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia.
6. Bapak Dekar Urumsah, S.E., S.Si., M.Com.(IS)., Ph.D., CFrA selaku Ketua Jurusan Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, dan selaku dosen pembimbing tesis yang telah bersedia meluangkan waktu serta memberikan ilmu, masukan, dan motivasi dengan penuh kesabaran kepada penulis selama proses penyusunan penelitian ini.
7. Bapak Arief Rahman, S.E., S.I.P., M.Com., Ph.D selaku Ketua Program Studi Magister Akuntansi Universitas Islam Indonesia.
8. Seluruh dosen Program Magister Akuntansi Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia atas ilmu yang telah diberikan sehingga dapat bermanfaat bagi peneliti dan menjadi bekal dalam pembuatan penelitian ini.
9. Seluruh responden yang telah berkenan meluangkan waktu untuk mengisi kuesioner sehingga peneliti dapat menyelesaikan penelitian ini.
10. Seluruh pihak yang tidak bisa disebutkan satu persatu, yang telah memberikan bantuan kepada penulis dalam menyelesaikan penelitian ini.

Semoga apa yang telah diberikan kepada penulis, menjadi amal ibadah yang diterima di sisi Allah SWT dan semoga Allah meridhoi dan mengabulkan doa dan harapan kita. Aamiin.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Yogyakarta, Juli 2023

Hanifah Zahra

ABSTRACT

This study aims to examine the factors influencing the financial cybercrime avoidance behavior among employees in the financial sector in Indonesia. The theories employed in this study are the Technology Threat Avoidance Theory (TTAT) and Regret Theory. The study uses a survey method by distributing questionnaires directly or indirectly to financial sector employees in Indonesia, with a total of 180 questionnaires collected for analysis. The data analysis employs the Structural Equation Modeling-Partial Least Squares (SEM-PLS) method using SmartPLS software. The research findings indicate that Perceived Susceptibility and Perceived Severity have a significant positive effect on Perceived Threat. However, there is no interaction between Perceived Susceptibility and Perceived Severity in influencing Perceived Threat. Perceived Threat, Safeguard Effectivity, and Anticipated Regret significantly influence the Motivation of Financial Cybercrime Avoidance. On the other hand, Self-Efficacy and Safeguard Cost do not affect the Motivation of Financial Cybercrime Avoidance. Moreover, the Motivation of Financial Cybercrime Avoidance has a significant positive influence on the Financial Cybercrime Avoidance Behavior. The implications of this research suggest that the results can be used as considerations by the government or regulators when formulating cybersecurity-related policies. Financial sector companies can also use the findings to determine appropriate actions to respond to cybercrime attacks. Furthermore, software protection developers (antivirus) can utilize the results to enhance software features.

Keywords: *Avoidance Behavior; Avoidance Motivation; Financial Cybercrime; Regret Theory; Technology Threat Avoidance Theory (TTAT).*

ABSTRAK

Penelitian ini bertujuan untuk menguji faktor-faktor yang mempengaruhi perilaku penghindaran kejahatan siber keuangan oleh pekerja sektor keuangan di Indonesia. Teori yang digunakan dalam penelitian ini adalah *Technology Threat Avoidance Theory* (TTAT) dan *Regret Theory*. Penelitian ini menggunakan metode survei dengan menyebar kuesioner secara langsung maupun tidak langsung kepada pekerja sektor keuangan di Indonesia. Terdapat 180 kuesioner yang dapat diolah pada penelitian ini. Pengujian data pada penelitian ini menggunakan metode SEM-PLS dengan software SmartPLS. Hasil penelitian ini menunjukkan bahwa Persepsi Kerentanan dan Persepsi Keparahan berpengaruh positif signifikan terhadap Persepsi Ancaman; tidak terdapat interaksi antara Persepsi Kerentanan dan Persepsi Keparahan dalam mempengaruhi Persepsi Ancaman; Persepsi Ancaman, Efektivitas Perlindungan, dan Antisipasi Penyesalan berpengaruh positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan; Efikasi Diri dan *Safeguard Cost* tidak berpengaruh terhadap Motivasi Penghindaran Kejahatan Siber Keuangan; dan Motivasi Penghindaran Kejahatan Siber Keuangan berpengaruh positif signifikan terhadap Perilaku Penghindaran Kejahatan Siber Keuangan. Implikasi dari penelitian ini adalah hasil penelitian ini dapat digunakan sebagai pertimbangan oleh pemerintah atau regulator dalam merumuskan kebijakan terkait keamanan siber; perusahaan sektor keuangan dalam menentukan tindakan-tindakan yang tepat untuk merespon serangan kejahatan siber; serta pengembang perangkat lunak perlindungan (antivirus) dalam mengembangkan fitur perangkat lunak.

Kata Kunci: Kejahatan Siber Keuangan; Motivasi Penghindaran; Perilaku Penghindaran; *Regret Theory; Technology Threat Avoidance Theory* (TTAT).

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era digital seperti saat ini, kehidupan manusia semakin erat dengan perkembangan teknologi siber. Ruang siber atau *cyberspace* patut mendapatkan perhatian dari seluruh pengguna teknologi siber. Ruang siber adalah sistem elektronik yang tersambung dengan internet hingga membentuk suatu ruang baru di luar ruang fisik seperti darat, laut, dan udara, di mana di dalamnya terbentuk interaksi dan ekosistem sosial dan ekonomi secara digital. Para pengguna teknologi siber harus memiliki kesadaran untuk menciptakan keamanan dan kenyamanan ruang siber agar ancaman siber tidak menimbulkan kerugian besar dan menyebabkan sesuatu yang fatal. Ruang siber yang aman adalah ruang siber yang tidak terkontaminasi kejahatan siber. Semakin tinggi tingkat pemanfaatan teknologi informasi dan komunikasi dalam ruang siber akan berbanding lurus dengan risiko dan ancaman keamanannya (Giyanto, 2021). Dengan adannya kesadaran pengguna teknologi dalam menciptakan keamanan dan kenyamanan ruang siber, maka akan meminimalkan keberhasilan tindakan kejahatan siber.

Kejahatan siber atau *cyber crime* merupakan tindak kejahatan yang dilakukan melalui jaringan internet. *Cyber crime* juga dapat diartikan sebagai eksploitasi yang disengaja terhadap sistem komputer, perusahaan yang bergantung pada teknologi, dan jaringan (Jenab & Moslehpour, 2016). Beberapa literatur mendefinisikan *cybercrime* merupakan tindakan yang identik dengan *computer crime.* Menurut the U.S. Department of Justice, *computer crime* merupakan

tindakan ilegal yang membutuhkan pengetahuan di bidang teknologi komputer untuk perbuatannya, penyelidikannya, dan penuntutannya. Sedangkan menurut *Organization for Economic Cooperation Development* (OECD), *computer crime* merupakan tindakan yang ilegal atau tidak etis atau tidak sah yang berkaitan dengan pemrosesan data otomatis dan/atau transmisi data.

Ruang lingkup kejahatan siber meliputi aktivitas pembajakan, penipuan, pencurian, pornografi, pelecehan, pemfitnahan, dan pemalsuan (Maskun, 2014). Beberapa bentuk kejahatan siber dapat berupa sekumpulan program komputer yang dapat mengganggu perilaku normal sistem komputer (virus), perangkat lunak berbahaya *(malware),* e-mail yang tidak diminta *(spam),* perangkat lunak pemantauan *(spyware),* percobaan membuat sumber daya komputer tidak tersedia untuk pengguna yang dituju *(DDoS attack),* seni peretasan/rekayasa manusia *(social engineering),* dan pencurian identitas online *(phishing)*. Berbagai kejahatan siber tersebut disiapkan untuk menargetkan keuntungan keuangan dan sosial (Ng, *et al.,* 2009). Sedangkan *financial cyber crime* yang dimaksud dalam penelitian ini adalah segala bentuk kejahatan yang dilakukan dalam sistem berbasis komputer atau jaringan internet untuk memanipulasi informasi keuangan atau mencuri uang korban sehingga menimbulkan kerugian secara keuangan.

Tindakan kejahatan siber di Indonesia marak terjadi. Badan Siber dan Sandi Negara (BSSN) menyebut lebih dari 700 juta serangan siber terjadi di Indonesia pada tahun 2022. Serangan siber yang mendominasi adalah *ransomware* atau *malware* dengan modus meminta tebusan. Selain *ransomware*, terdapat juga serangan siber yang menggunakan metode *phishing* dan eksploitasi kerentanan di

peringkat dua dan tiga. Maraknya tindakan kejahatan siber berbanding lurus dengan frekuensi masyarakat dalam menggunakan internet. Berdasarkan hasil survei yang dirilis oleh (We Are Social Hootsuite, 2022), jumlah pengguna internet di Indonesia mencapai 204,7 juta orang atau 73,7% dari total jumlah penduduk Indonesia. Penelitian tersebut juga menyatakan bahwa masyarakat Indonesia mayoritas mengakses internet dengan menggunakan *mobile phone* dan komputer personal atau laptop dengan waktu akses rata-rata 8 jam 36 menit. Tingginya penggunaan internet oleh masyarakat Indonesia, tidak berbanding lurus dengan tingkat keamanan siber di Indonesia. Berdasarkan laporan yang dirilis oleh (NCSI, 2022), Indonesia berada di peringkat 84 dari 161 negara dalam hal keamanan siber dengan skor 38,96 dari 100. Hal tersebut menunjukkan bahwa tingkat keamanan siber di Indonesia masih rendah.

Tingkat keamanan siber yang rendah, merupakan sebuah tantangan bagi perusahaan-perusahaan yang kini telah melakukan transformasi digital dalam proses operasional bisnisnya. Salah satu tantangan perusahaan dalam penggunaan teknologi adalah perusahaan tidak mampu meningkatkan tingkat keamanan data untuk menjaga dan melindungi informasi mengenai para pemangku kepentingan dan perusahaan itu sendiri dengan lebih efektif (Gupta et al., 2020). Dilansir dari laporan survei kejahatan dan penipuan ekonomi global yang dirilis oleh PWC pada tahun 2022, di seluruh organisasi dari semua ukuran, *cybercrime* menimbulkan ancaman terbesar, diikuti oleh *customer fraud* dan *assets misappropriation*. Selain itu, survei tersebut juga mengidentifikasi bahwa permainan *fraud* telah berubah dari sebelumnya. Profil ancaman utama muncul dari entitas eksternal yang tidak dapat

dikendalikan oleh perusahaan. Data survei tersebut menunjukan bahwa secara global 43% pelaku *fraud* berasal dari entitas eksternal, 31% berasal dari entitas internal, dan 26% pelaku *fraud* melakukan kolusi antara entitas internal dan eksternal. *Fraud* yang dilakukan oleh entitas eksternal, sekitar 33% merupakan tindakan peretasan dan 28% merupakan tindakan kejahatan terorganisir (PwC, 2022).

Pada tahun 2022, serangan siber terbesar merupakan serangan terhadap sektor manufaktur sebesar 23,2%, diikuti oleh sektor keuangan sebesar 22,4%, sektor pelayanan bisnis sebesar 12,7%, sektor energi sebesar 8,2%, sektor perdagangan sebesar 7,3%, sektor kesehatan sebesar 5,1%, sektor transportasi sebesar 4%, sektor pemerintahan sebesar 2,8%, sektor pendidikan sebesar 2,8%, dan sektor media sebesar 2,5% (IBM, 2022). Menurut IBM, 95% keberhasilan serangan siber disebabkan oleh kesalahan manusia. Persentase kesalahan manusia atau *human error* dalam hal keamanan siber cukup besar, 19 dari 20 pelanggaran dunia maya diakibatkan oleh kelalaian manusia. *Human error* yang dimaksud mencakup aktivitas seperti mengunduh perangkat lunak yang terinfeksi, menyimpan kata sandi yang lemah, dan tidak memperbarui perangkat lunak. Manusia atau pengguna komputer memang memainkan peran paling penting dalam menciptakan dunia maya yang lebih aman dalam pertumbuhan teknologi internet. Teknologi internet begitu meresap saat ini sehingga menjadi tumpuan untuk kehidupan modern yang memungkinkan orang biasa berbelanja, bersosialisasi, dan dihibur melalui komputer mereka sendiri. Seiring ketergantungan orang pada internet terus meningkat, kemungkinan peretasan dan pelanggaran keamanan

lainnya turut meningkat secara teratur (Liang & Xue, 2010). Maka dari itu perlu dilakukan penelitian terkait perilaku penghindaran serangan kejahatan siber keuangan.

Perilaku memiliki makna strategi dan solusi (Klein et al., 2000) serta memiliki makna "selalu melakukan" dan "biasa melakukan" (Oz et al., 2013). Berdasarkan makna tersebut, perilaku penghindaran dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menghindari suatu hal. Perilaku penghindaran dapat didefinisikan sebagai perilaku apapun yang dilakukan dengan tujuan mengalihkan diri dari situasi yang tidak diinginkan (Sheynin et al., 2014). Dari definisi yang telah disebutkan, maka perilaku penghindaran kejahatan siber keuangan dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menghindari serangan kejahatan siber keuangan yang menyerang dirinya.

Penelitian sebelumya terkait perilaku penghindaran kejahatan siber juga telah dilakukan oleh peneliti sebelumnya dengan menggunakan beberapa teori yang telah ada seperti *Technology Threat Avoidance Theory* dan *Protection Motivation Theory*. Teori *Technology Threat Avoidance Theory* telah digunakan oleh (Verkijika, 2019), Sylvester (2022), Saidi & Prayudi (2021), Mark et al., (2021), dan Gillam & Foster (2020). Sedangkan teori *Protection Motivation Theory* telah digunakan oleh Tang et al., (2021) dan Bax et al., (2021).

Penelitian menggunakan teori TTAT yang dilakukan oleh(Verkijika, 2019) menunjukkan bahwa efikasi diri berpengaruh positif terhadap motivasi penghindaran *phishing* dan motivasi penghindaran *phishing* berpengaruh terhadap

perilaku penghindaran *phishing*. Sedangkan hasil penelitian lain oleh Sylvester (2022) menunjukan bahwa persepsi kerentanan, persepsi keparahan, persepsi ancaman, efikasi diri, efektivitas perlindungan, *safeguard cost*, dan motivasi penghindaran berpengaruh positif terhadap perilaku penghindaran *phishing.* Penelitian lainnya yang dilakukan oleh Saidi & Prayudi (2021) menunjukkan bahwa terdapat keterkaitan antar faktor yang sangat berpengaruh terhadap perilaku penghindaran serangan *phishing* yaitu faktor *behavioral intention* dengan faktor efikasi diri. Hasil penelitian lain oleh Mark et al., (2021) menunjukkan bahwa interkasi antara persepsi kerentanan dan persepsi keparahan berpengaruh positif terhadap persepsi ancaman; persepsi ancaman, efektivitas perlindungan, dan efikasi diri berpengaruh terhadap motivasi penghindaran ancaman kejahatan teknologi informasi; dan motivasi penghindaran ancaman kejahatan teknologi informasi berpengaruh positif terhadap perilaku penghindaran ancaman kejahatan teknologi informasi. Penelitian lain menggunakan teori TTAT yang dilakukan oleh Gillam & Foster (2020) membuktikan bahwa persepsi kerentanan, *safeguard cost*, dan efikasi diri berpengaruh terhadap perilaku penghindaran kejahatan siber.

Berdasarkan penelitian yang telah dilakukan tersebut, peneliti menggunakan kerangka TTAT dengan konstruksi persepsi kerentanan, persepsi keparahan, persepsi ancaman, efikasi diri, *safeguard cost*, dan motivasi penghindaran kejahatan siber keuangan sebagai faktor yang dapat mempengaruhi perilaku penghindaran kejahatan siber keuangan. Peneliti memperluas model penelitian dengan menambahkan konstruk *anticipated regret* yang dirumuskan dari teori penyesalan.

Persepsi kerentanan atau *perceived susceptibility* merupakan keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik (Liang & Xue, 2010). Berdasarkan penelitian mengenai pengaruh persepsi kerentanan terhadap perilaku penghindaran kejahatan siber keuangan, persepsi kerentanan memberikan pengaruh secara tidak langsung terhadap perilaku penghindaran kejahatan siber keuangan melalui persepsi ancaman. Dalam penelitian yang dilakukan oleh (Arachchilage et al., 2016); (Gillam & Foster, 2020); (Mark et al., 2021); (Saidi & Prayudi, 2021); dan (Sylvester, 2022) menunjukkan bahwa persepsi kerentanan berpengaruh positif terhadap persepsi ancaman.

Persepsi keparahan atau *perceived severity* merupakan keyakinan individu mengenai keparahan yang dirasakan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber (Liang & Xue, 2010). Penelitian yang dilakukan oleh (Arachchilage et al., 2016); (Mark et al., 2021); (Saidi & Prayudi, 2021); dan (Sylvester, 2022) membuktikan bahwa persepsi keparahan berpengaruh positif terhadap persepsi ancaman, sedangkan penelitian oleh (Gillam & Foster, 2020) menunjukkan bahwa persepsi keparahan tidak berpengaruh terhadap persepsi ancaman.

Persepsi ancaman atau *perceived threat* merupakan keyakinan individu akan menjadi korban ancaman teknologi informasi (Liang & Xue, 2009a). Menurut teori *Technology Threat Avoidance Theory* yang dikembangkan oleh (Liang & Xue,

2009a), persepsi ancaman akan berpengaruh secara tidak langsung terhadap perilaku penghindaran kejahatan siber. Persepsi anacaman akan berpengaruh terhadap perilaku penghindaran kejahatan siber melalui motivasi penghindaran. Dalam penelitian yang terkait dengan persepsi ancaman, penelitian yang dilakukan oleh Mark et al., (2021) menunjukkan bahwa persepsi ancaman memiliki pengaruh positif terhadap perilaku penghindaran terhadap tindakan *phishing*. Sedangkan dalam penelitian oleh Djatsa (2020) menunjukkan bahwa persepsi ancaman tidak berpengaruh terhadap perilaku penghindaran terhadap kejahatan siber.

Efikasi diri diartikan sebagai persepsi seseorang atas keterampilan dan kemampuan dirinya untuk melakukan perilaku perlindungan tertentu (Verkijika, 2019). Efikasi diri juga dapat diartikan sebagai kepercayaan individu akan kemampuannya untuk sukses dalam melakukan sesuatu (Bandura, 1986). Efikasi diri merupakan penentu penting dari motivasi penghindaran. Hasil dari penelitian yang dilakukan oleh (Verkijika, 2019) menunjukkan bahwa efikasi diri berpengaruh positif terhadap motivasi dan perilaku penghindaran atas serangan *phishing.* Hasil tersebut sejalan dengan penelitian yang dilakukan oleh (Tang et al., 2021);(Saidi & Prayudi, 2021); (Mark et al., 2021); (Gillam & Foster, 2020); dan Arachchilage *et al.,* (2016) yang dalam penelitiannya menunjukkan bahwa efikasi diri berpengaruh terhadap perilaku penghindaran kejahatan siber.

Efektivitas perlindungan didefinisikan sebagai penilaian individu dari tindakan pengamanan mengenai seberapa efektif hal itu dapat diterapkan untuk menghindari ancaman teknologi informasi yang berbahaya (Liang & Xue, 2010). Misalnya, penilaian individu mengenai seberapa efektif pendidikan *anti-phishing*

dapat diterapkan untuk menghindari serangan *phishing*. Dalam penelitian yang dilakukan oleh Butler, (2020) dan (Arachchilage et al., 2016) membuktikan bahwa efektivitas perlindungan berpengaruh terhadap motivasi penghindaran kejahatan siber.

Safeguard cost didefinisikan sebagai upaya fisik dan kognitif seperti waktu, uang, ketidaknyamanan dan pemahaman yang diperlukan dengan menggunakan tindakan pengamanan (Liang & Xue, 2009a). Dalam penelitian yang dilakukan oleh Butler (2020) menunjukkan bahwa perhitungan biaya berpengaruh terhadap perilaku penghindaran. Hal tersebut sejalan dengan hasil penelitian oleh Gillam & Foster (2020) yang menunjukkan bahwa biaya yang dibutuhkan dalam melakukan perlindungan terhadap kejahatan siber berpengaruh terhadap perilaku penghindaran kejahatan siber. Sedangkan penelitian yang dilakukan oleh (Arachchilage et al., 2016) membuktikan bahwa *safeguard cost* tidak berpengaruh terhadap perilaku penghindaran tindakan *phishing*.

Antisipasi penyesalan didefinisikan sebagai respon afektif negatif yang diharapkan yang akan dialami pengguna teknologi jika individu gagal mengambil tindakan perlindungan yang diperlukan terhadap ancaman teknologi informasi (Liang & Xue, 2018). *Anticipated regret* juga dapat diartikan sebagai penyesalan tindakan atau penyesalan tidak bertindak. Penyesalan tindakan mencakup penyesalan yang dihasilkan dari terlibat dalam perilaku tertentu sementara penyesalan tidak bertindak dihasilkan dari kegagalan individu untuk terlibat dalam perilaku tertentu (Brewer et al., 2016). Menurut(Sukamulja et al., 2019), *anticipated regret* muncul ketika hasil dari suatu proses yang telah melewati proses

perencanaan, ternyata tidak sesuai dengan yang diharapkan. Dalam penelitian ini, fokusnya adalah penyesalan kelambanan pengambilan keputusan untuk menghindari serangan terhadap teknologi informasi. Hal ini karena ketika menghadapi ancaman keamanan informasi, hasil negatif yang mengarah pada penyesalan cenderung lebih besar apabila seseorang gagal mengambil keputusan. Penelitian sebelumnya yang dilakukan oleh (Verkijika, 2019) telah membuktikan bahwa penyesalan yang diantisipasi berpengaruh positif terhadap motivasi penghindaran kejahatan siber.

Motivasi penghindaran atau *avoidance motivation* didefinisikan sebagai seberapa termotivasi pengguna untuk menghindari ancaman TI dengan melakukan atau menggunakan ukuran atau metode pengamanan (Liang & Xue, 2010). Berdasarkan teori *Technology Threat Avoidance Theory* yang dikembangkan oleh (Liang & Xue, 2009a), perilaku penghindaran ancaman teknologi informasi ditentukan oleh motivasi penghindaran ancaman teknologi informasi. Dalam penelitian yang dilakukan oleh (Verkijika, 2019); (Mark et al., 2021); (Butler, 2020); (Gillam & Foster, 2020); dan Arachchilage, *et al.*, (2016) membuktikan bahwa motivasi penghindaran kejahatan siber berpengaruh positif terhadap perilaku penghindaran kejahatan siber.

Tinjauan literatur sebelumnya menunjukkan bahwa sebagian besar penelitian dilakukan berkaitan dengan perilaku penghindaran tindakan *phishing* (Verkijika (2019); Sylvester (2022); Saidi & Prayudi (2021); Mark et al., (2021); Bax et al., (2021)). Dalam penelitian oleh Verkijika (2019) terdapat keterbatasan, yaitu variabel yang diadopsi dari *Technology Threat Avoidance Theory* hanyalah

variabel efikasi diri atau *self-efficacy.* Berdasarkan hasil penelitian yang telah dilakukan, Verkijika (2019) menyarankan bagi peneliti selanjutnya untuk mempertimbangkan faktor-faktor lain selain efikasi diri seperti persepsi kerentanan, persepsi keparahan, *safeguard cost,* dan efektivitas perlindungan untuk mengevaluasi pengaruh mereka pada perilaku penghindaran ancaman kejahatan siber karena faktor-faktor tersebut diketahui memainkan peran penting dalam meningkatkan motivasi atau niat penghindaran keamanan.

Berdasarkan hal tersebut, penelitian ini menggunakan konstruksi dalam kerangka TTAT dan menambahkan konstruksi antisipasi penyesalan yang berasal dari kerangka teori penyesalan atau *regret theory.* Penambahan konstruksi tersebut dilandasi oleh teori penyesalan yang berpendapat bahwa dalam setiap keputusan yang diambil oleh seseorang pasti selalu ada unsur penyesalan. Dengan demikian, seseorang sering mengantisipasi penyesalan yang mungkin akan mereka alami akibat terlibat dalam suatu perilaku tertentu dan kemudian bertindak dengan cara yang dapat meminimalkan penyesalan (Shih & Schau, 2011). Pandangan ini telah didukung dalam literatur penghindaran serangan *phishing* dimana terlihat bahwa penyesalan yang diantisipasi secara positif berpengaruh terhadap perilaku penghindaran serangan *phishing* oleh pekerja di Afrika.

Penelitian ini menarik dilakukan karena penelitian yang serupa khususnya di Indonesia masih jarang dilakukan. Selain itu, penelitian-penelitian sebelumnya yang dilakukan oleh Verkijika (2019); Sylvester (2022); Saidi & Prayudi (2021); Mark et al., (2021); Bax et al., (2021) masih menunjukkan hasil yang inkonsisten untuk setiap variabelnya. Penelitian yang memiliki hasil inkonsisten menarik untuk

dilakukan penelitian ulang. Berdasarkan hal tersebut, peneliti tertarik untuk melakukan penelitian yang berjudul "Determinan Perilaku Penghindaran Kejahatan Siber Keuangan oleh Pekerja Sektor Keuangan di Indonesia".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, adapun rumusan masalah pada penelitian ini antara lain:

1. Apakah persepsi kerentanan berpengaruh terhadap persepsi ancaman?
2. Apakah persepsi keparahan berpengaruh terhadap persepsi ancaman?
3. Apakah interaksi antara persepsi kerentanan dan persepsi keparahan berpengaruh terhadap persepsi ancaman?
4. Apakah persepsi ancaman berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan?
5. Apakah *safeguard cost* berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan?
6. Apakah efikasi diri berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan?
7. Apakah efektivitas perlindungan berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan?
8. Apakah antisipasi penyesalan berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan?
9. Apakah motivasi penghindaran serangan siber keuangan berpengaruh terhadap perilaku penghindaran kejahatan siber keuangan?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas maka tujuan penelitian yang hendak dicapai dalam penelitian ini adalah:

1. Untuk mengetahui dan menganalisis pengaruh persepsi kerentanan terhadap persepsi ancaman.
2. Untuk mengetahui dan menganalisis pengaruh persepsi keparahan terhadap persepsi ancaman.
3. Untuk mengetahui dan menganalisis pengaruh interaksi antara persepsi kerentanan dan persepsi keparahan terhadap persepsi ancaman.
4. Untuk mengetahui dan menganalisis pengaruh persepsi ancaman terhadap motivasi penghindaran serangan siber keuangan.
5. Untuk mengetahui dan menganalisis pengaruh *safeguard cost* terhadap motivasi penghindaran serangan siber keuangan.
6. Untuk mengetahui dan menganalisis pengaruh efikasi diri terhadap motivasi penghindaran serangan siber keuangan.
7. Untuk mengetahui dan menganalisis pengaruh efektivitas perlindungan terhadap motivasi penghindaran kejahatan siber keuangan.
8. Untuk mengetahui dan menganalisis pengaruh antisipasi penyesalan terhadap motivasi penghindaran kejahatan siber keuangan.
9. Untuk mengetahui dan menganalisis pengaruh motivasi penghindaran kejahatan siber keuangan terhadap perilaku penghindaran kejahatan siber keuangan.

1.4 Manfaat Penelitian

Penelitian ini memiliki manfaat bagi berbagai pihak, diantaranya:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat berkontribusi terhadap wacana teoritis yang berhubungan dengan perilaku penghindaran kejahatan siber keuangan. Serta diharapkan mampu memberikan wawasan mengenai tindakan kejahatan siber keuangan serta upaya menghindarinya.

2. Manfaat Praktis

   Penelitian ini diharapkan mampu berkontribusi dalam ranah praktis terhadap berbagai pihak yaitu regulator, pengembang sistem keamanan siber, dan pengguna teknologi informasi.

   a. Bagi Regulator

      Penelitian ini diharapkan dapat berkontribusi bagi regulator untuk mempertimbangkan pengembangan aturan hukum terkait keamanan siber di Indonesia.

   b. Bagi Pengembang Sistem Keamanan Siber

      Penelitian ini diharapkan dapat berkontribusi bagi pengembang sistem keamanan siber untuk mempertimbangkan perilaku penghindaran kejahatan siber oleh pengguna teknologi di Indonesia dalam mengembangkan sistemnya.

c. Bagi Pengguna Teknologi Informasi

Penelitian ini diharapkan dapat berkontribusi bagi pengguna teknologi informasi dalam hal mengambil keputusan dalam hal merespon atau menghindari kejahatan siber keuangan.

1.5 Sistematika Penulisan

Penelitian ini terdiri atas lima bab yang tersusun secara sistematis dengan sistematika sebagai berikut:

BAB I: Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian serta sistematika penulisan.

BAB II: Tinjauan Pustaka

Bab ini berisi tentang landasan teoritik model penelitian, latar belakang teoritik dari literatur-literatur serta hasil-hasil penelitian sebelumnya yang mendasari argumentasi pemilihan variable. Dalam bab ini diterangkan pula alur teoritik pengembangan hipotesis.

BAB III: Metode Penelitian

Bab ini berisi tentang definisi serta deskripsi operasional variabel-variabel penelitian, penentuan populasi dan sampel, jenis dan sumber data, metode pengumpulan data, dan metode analisis data.

BAB IV: Hasil Pembahasan

Bab ini berisi tentang deskripsi objek penelitian, analisis data, hasil pengujian hipotesis, diakhiri dengan interpretasi serta diskusi hasil penelitian.

BAB V: Kesimpulan dan Saran

Bab ini berisi kesimpulan akhir atas hasil analisis pada bab sebelumnya dilanjutkan dengan pemaparan implikasi hasil penelitian dan saran-saran bagi berbagai pihak yang berkepentingan.

BAB 2

KAJIAN PUSTAKA

2.1 Landasan Teori

2.1.1 *Technology Threat Avoidance Theory (TTAT)*

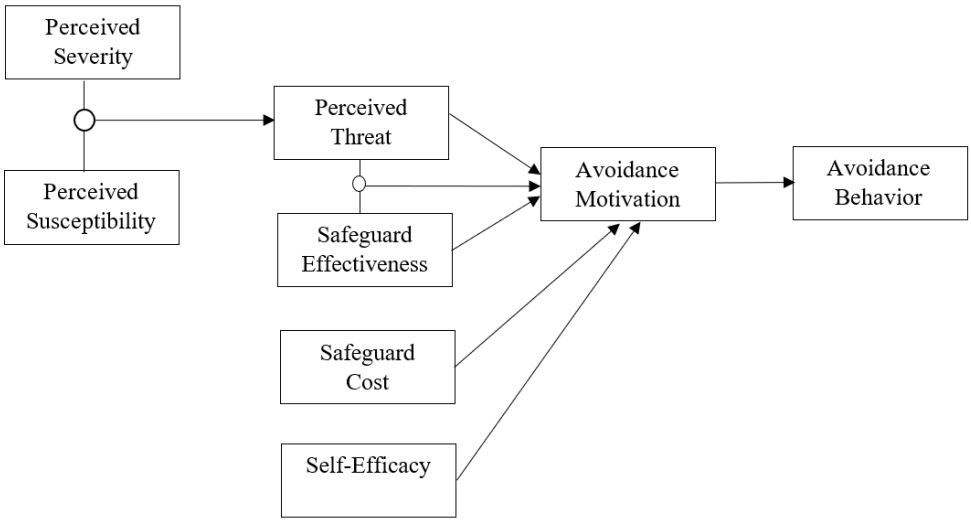
Technology Threat Avoidance Theory merupakan teori yang dikembangkan oleh (Liang & Xue, 2009a) yang menjelaskan perilaku seseorang terhadap perlindungan jaringan dalam hal motivasi untuk menghindari ancaman terhadap jaringan atau komputer yang digunakan. TTAT dikembangkan dengan mengintegrasikan beberapa model teoritis yang telah ada, yaitu *cybernetics theory* yang dirumuskan oleh Wiener (1948), *coping theory* oleh Lazarus (1966), teori motivasi perlindungan atau *protection motivation theory* oleh Rogers (1975), *health belief model* oleh Janz dan Becker (1984), dan *risk analysis research model* oleh Baskerville (1991).

TTAT berpendapat bahwa dalam konteks tertentu, persepsi ancaman terbentuk berdasarkan persepsi mereka terhadap tingkat keparahan yang terkait dengan ancaman kejahatan dunia maya tertentu dan persepsi atas kerentanan mereka sendiri terhadap ancaman kejahatan dunia maya. Dengan meyakini persepsi ancaman, seseorang kemudian akan menilai kemampuan mereka untuk mengatasi ancaman tersebut berdasarkan hal-hal berikut ini:

1. Seberapa efektif mereka percaya dengan perlindungan yang diberikan untuk menghindari ancaman kejahatan siber,
2. Seluruh upaya yang diperlukan dalam upaya penerapan perlindungan untuk menghindari ancaman kejahatan dunia maya, dan

3. Kemampuan mereka untuk menerapkan perlindungan untuk menghindari ancaman kejahatan dunia maya.

Keluaran dari proses penilaian ini merupakan tingkat tertentu dari motivasi penghindaran kejahatan dunia maya, yang pada gilirannya akan mempengaruhi keputusan individu untuk terlibat dalam perilaku yang secara khusus dimaksudkan untuk membantu mereka menghindari ancaman kejahatan dunia maya. Berikut ini merupakan diagram model *Technology Threat Avoidance Theory* yang dikembangkan oleh (Liang & Xue, 2009b).



Gambar 2.1 *Technology Threat Avoidance Theory*

Perceived Severity atau persepsi keparahan didefinisikan sebagai keyakinan individu mengenai persepsi keparahan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber. *Perceived susceptibility* atau persepsi kerentanan didefinisikan sebagai keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik. Persepsi ancaman

atau *perceived threat* didefinisikan sebagai keyakinan individu akan menjadi korban ancaman teknologi informasi. *Safeguard effectiveness* atau efektivitas perlindungan didefinisikan sebagai penilaian individu dari tindakan pengamanan mengenai seberapa efektif hal itu dapat diterapkan untuk menghindari ancaman teknologi informasi yang berbahaya. *Safeguard cost* didefinisikan sebagai upaya fisik dan kognitif seperti waktu, uang, ketidaknyamanan dan pemahaman yang diperlukan dengan menggunakan tindakan pengamanan. Efikasi diri atau *self efficacy* merupakan keyakinan individu dalam mengambil tindakan pengamanan. Motivasi penghindaran atau *avoidance motivation* didefinisikan sebagai seberapa termotivasi pengguna untuk menghindari ancaman teknologi informasi dengan melakukan atau menggunakan ukuran atau metode pengamanan (Liang dan Xue, 2009).

2.1.2 *Regret Theory*

Regret Theory atau teori penyesalan merupakan sebuah model dalam teori ekonomi yang dikembangkan secara bersamaan oleh (Loomes & Sugden, 1982); (Bell, 1982); dan (Fishburn, 1982). Model teori ini menjelaskan terkait penyesalan di bawah ketidakpastian dengan mempertimbangkan efek penyesalan yang diantisipasi. Menurut (Bell, 1982) serta (Loomes & Sugden, 1982), teori penyesalan dibangun berdasarkan dua asumsi. Pertama, pada dasarnya seseorang cenderung membandingkan antara hasil (*outcome*) dari keputusannya memilih dengan hasil dari apa yang mereka akan terima seandainya melakukan pilihan yang berbeda. Kedua, individu cenderung mengantisipasi penyesalan sebelum membuat keputusan, karenanya seringkali mereka mengubah pilihan untuk menghindari

potensi penyesalan. *Anticipated regret* juga dapat diartikan sebagai penyesalan tindakan atau penyesalan tidak bertindak. Penyesalan tindakan mencakup penyesalan yang dihasilkan dari terlibat dalam perilaku tertentu sementara penyesalan tidak bertindak dihasilkan dari kegagalan individu untuk terlibat dalam perilaku tertentu (Brewer et al., 2016). Menurut (Sukamulja et al., 2019), *anticipated regret* muncul ketika hasil dari suatu proses yang telah melewati proses perencanaan, ternyata tidak sesuai dengan yang diharapkan.

2.1.3 Kejahatan Siber Keuangan

Kejahatan siber atau *cyber crime* merupakan tindak kejahatan yang dilakukan melalui jaringan internet. *Cyber crime* juga dapat diartikan sebagai eksploitasi yang disengaja terhadap sistem komputer, perusahaan yang bergantung pada teknologi, dan jaringan (Jenab & Moslehpour, 2016). Beberapa literatur mendefinisikan *cybercrime* merupakan tindakan yang identik dengan *computer crime.* Menurut the *U.S. Department of Justice*, *computer crime* merupakan tindakan ilegal yang membutuhkan pengetahuan di bidang teknologi komputer untuk perbuatannya, penyelidikannya, dan penuntutannya. Sedangkan menurut *Organization for Economic Cooperation Development* (OECD), *computer crime* merupakan tindakan yang ilegal atau tidak etis atau tidak sah yang berkaitan dengan pemrosesan data otomatis dan/atau transmisi data.

Ruang lingkup kejahatan siber meliputi pembajakan, penipuan, pencurian, pornografi, pelecehan, pemfitnahan, dan pemalsuan (Maskun, 2014). Dari penipuan hingga pemalsuan, *spoofing* hingga *spamming*, penjahat dunia maya secara khusus menargetkan uang sebagai target utamanya. Laporan menunjukkan

bahwa, setiap tahun, rincian keuangan jutaan orang dicuri dari sistem yang dioperasikan oleh hotel, rantai ritel, bank, dan penyedia layanan masyarakat.

Financial cyber crime yang dimaksud dalam penelitian ini adalah kejahatan yang dilakukan dalam sistem berbasis komputer atau jaringan internet untuk memanipulasi informasi keuangan atau menargetkan uang korban sebagai target utamanya sehingga menimbulkan kerugian secara keuangan. Menurut (The World Bank and the United Nations, 2017), bentuk kejahatan siber yang dapat mengakibatkan kerugian secara finansial merupakan kejahatan-kejahatan berikut ini:

1. *Hacking*

   Hacking merupakan kejahatan siber yang paling mendasar karena memungkinkan perilaku kriminal (siber) selanjutnya. Setelah akses diperoleh ke perangkat atau jaringan komputer, pelaku kejahatan siber dapat menargetkan informasi dan data, atau mungkin beralih ke sistem target. Ada berbagai cara untuk menyusup ke perangkat, sistem, atau jaringan. Tindakan *hacking* atau peretasan dapat dilakukan dengan berbagai cara, yaitu sebagai berikut:

   a. *Malware*

      Malware merupakan kode berbahaya (termasuk virus, worm, trojan, atau spyware) yang menginfeksi perangkat atau sistem, yang biasanya mampu menggandakan dirinya sendiri, dan biasanya memiliki efek merugikan, seperti merusak sistem atau menghancurkan data.

   b. *Adware*

Adware merupakan kode berbahaya yang mengunduh atau menampilkan iklan yang tidak diinginkan saat pengguna online, mengumpulkan data pemasaran dan informasi lainnya tanpa sepengetahuan pengguna, atau mengalihkan permintaan pencarian ke situs web periklanan tertentu.

c. Rekayasa Sosial

Rekayasa sosial atau yang biasa disebut *social engineering* merupakan penggunaan komunikasi elektronik yang menipu, seperti email atau pesan media sosial, untuk tujuan penipuan, akses sistem, atau mengumpulkan informasi sensitif; bentuk rekayasa sosial yang paling umum termasuk *phishing, pretexting, baiting, quid pro quo* dan *tailgating*.

d. Botnet

Botnet merupakan serangan terhadap jaringan komputer pribadi yang menginfeksi perangkat lunak jahat dan dikendalikan sebagai kelompok tanpa sepengetahuan pemiliknya untuk melipatgandakan efek serangan dunia maya.

e. *Denial-of-Service (DoS) atau Distributed Denial-of-Service (DDoS)*

DoS atau DDoS attack merupakan kejahatan siber yang bertujuan untuk membanjiri atau membebani situs web atau jaringan organisasi agar tidak tersedia bagi pengguna yang dituju dengan mengganggu atau menangguhkan layanan.

f. Ransomware

Ransomware berupa kode berbahaya yang disamarkan sebagai file sah yang digunakan oleh peretas untuk mengenkripsi data di perangkat

pengguna, sehingga mencegah akses ke data atau ke perangkat itu sendiri hingga biaya tebusan dibayarkan. Kebalikan dari serangan DoS, ransomware membuat pengguna tidak mungkin mendekripsi datanya sendiri tanpa kunci dekripsi, yang (pada prinsipnya) ditawarkan setelah pembayaran uang tebusan.

g. Serangan Injeksi

Jenis serangan yang paling umum dan sukses di internet (mis. SQL Injection (SOL), Cross-Site Scripting (XSS)), ini menargetkan aplikasi berbasis web, dan bekerja dengan menyembunyikan kode berbahaya ("muatan") di dalam input pengguna yang diverifikasi (dengan demikian melewati mekanisme otentikasi dan otorisasi) yang ditampilkan ke browser pengguna akhir, yang pada gilirannya mengeksekusi skrip yang tampaknya dapat dipercaya. Skrip sering membuat kesalahan yang terlihat oleh penyerang, banyak di antaranya cenderung cukup deskriptif untuk memungkinkan penyerang mendapatkan informasi tentang struktur database dan dengan demikian mengontrolnya.

2. *Data Forgery*

Data forgery merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

3. *Unauthorized Monitoring*

Unauthorized monitoring merupakan "pemantauan" yang tidak sah yang menargetkan perangkat, data, atau keduanya; ketika data ditargetkan, ini sering disebut sebagai "intersepsi ilegal". Kegiatan tersebut biasanya dilakukan dengan menggunakan atau memasang perangkat pemantauan atau perangkat lunak dalam sistem komputer setelah memperoleh akses ke sistem. Tindak kejahatan ini dapat dilakukan untuk memantau data-data rahasia organisasi pesaing.

Serangan siber terhadap sektor jasa keuangan dan perbankan di Indonesia terdiri dari berbagai bentuk/modus kejahatan (Suwiknyo *et al.,* 2021). Bentuk-bentuk kejahatan siber tersebut dijelaskan sebagai berikut:

1. Kejahatan *Carding* yaitu kejahatan siber berupa pembobolan data kartu kredit dan pelaku melakukan transaksi menggunakan data kartu kredit milik korban.
2. Pemerasan Siber yaitu kejahatan siber dengan modus pelaku akan meminta uang sebagai tebusan atas data penting yang telah dicuri.
3. Serangan *Adware* yaitu kejahatan siber berupa iklan/pemberitahuan yang muncul tanpa izin atau email *spam* yang berisikan hadiah atau penawaran uang dalam jumlah yang tidak realistis.
4. Penipuan OTP yaitu kejahatan siber berupa pesan/telepon berisi permintaan OTP (*one-time password*) untuk verifikasi aplikasi atau *website*. Pada umumnya, pelaku akan menyamar menjadi pihak bank atau instansi tertentu.
5. Penipuan Link Palsu yaitu kejahatan siber dimana pelaku mengirimkan link palsu kepada korban dengan tujuan mencuri data rekening milik orang yang

mengakses tautan tersebut. (Contoh: kasus link palsu resi paket dan link palsu persetujuan perubahan kebijakan bank).

6. Penipuan pesan berisi APK yaitu kejahatan siber berupa pesan berisi APK (aplikasi android) yang terinfeksi *malware.* Ketika aplikasi tersebut terpasang pada perangkat elektronik milik korban, maka pelaku dapat mencuri data penting milik korban. (Contoh: pesan berisi APK yang berkedok undangan pernikahan digital).

Berdasarkan data yang dirilis oleh Statista Technology Market Outlook (2022), kejahatan siber yang terjadi di seluruh dunia pada tahun 2022 menghasilkan kerugian sebesar US $8,44 triliun atau setara dengan Rp. 132.000 triliun. Kejahatan siber keuangan dapat dilakukan terhadap individu maupun organisasi. Berdasarkan laporan survei kejahatan dan penipuan ekonomi global yang dirilis oleh PWC pada tahun 2022, di seluruh organisasi dari semua ukuran, *cybercrime* menimbulkan ancaman terbesar, diikuti oleh *customer fraud* dan *assets misappropriation*. Selain itu, survei tersebut juga mengidentifikasi bahwa permainan *fraud* telah berubah dari sebelumnya. Profil ancaman utama muncul dari entitas eksternal yang tidak dapat dikendalikan oleh perusahaan. Data survei tersebut menunjukan bahwa secara global 43% pelaku *fraud* berasal dari entitas eksternal, 31% berasal dari entitas internal, dan 26% pelaku *fraud* melakukan kolusi antara entitas internal dan eksternal. *Fraud* yang dilakukan oleh entitas eksternal, sekitar 33% merupakan tindakan peretasan dan 28% merupakan tindakan kejahatan terorganisir (PWC, 2022).

Pada tahun 2022, secara global serangan siber terbesar merupakan serangan terhadap sektor manufaktur sebesar 23,2%, diikuti oleh sektor keuangan sebesar 22,4%, sektor pelayanan bisnis sebesar 12,7%, sektor energi sebesar 8,2%, sektor perdagangan sebesar 7,3%, sektor kesehatan sebesar 5,1%, sektor transportasi sebesar 4%, sektor pemerintahan sebesar 2,8%, sektor pendidikan sebesar 2,8%, dan sektor media sebesar 2,5% (IBM, 2022).

Di Indonesia sendiri, Badan Siber dan Sandi Negara (BSSN) menyebut lebih dari 700 juta serangan siber terjadi di Indonesia pada tahun 2022. Serangan siber yang mendominasi adalah *ransomware* atau *malware* dengan modus meminta tebusan. Selain *ransomware*, terdapat juga serangan siber yang menggunakan metode *phishing* dan eksploitasi kerentanan di peringkat dua dan tiga. Berdasarkan hasil survei yang dirilis oleh (We Are Social Hootsuite, 2022), jumlah pengguna internet di Indonesia mencapai 204,7 juta orang atau 73,7% dari total jumlah penduduk Indonesia. Penelitian tersebut juga menyatakan bahwa masyarakat Indonesia mayoritas mengakses internet dengan menggunakan *mobile phone* dan komputer personal atau laptop dengan waktu akses rata-rata 8 jam 36 menit. Tingginya penggunaan internet oleh masyarakat Indonesia, tidak berbanding lurus dengan tingkat keamanan siber di Indonesia. Berdasarkan laporan yang dirilis oleh (NCSI, 2022), Indonesia berada di peringkat 84 dari 161 negara dalam hal keamanan siber dengan skor 38,96 dari 100.

2.1.4 Perilaku Penghindaran

Perilaku memiliki makna strategi dan solusi (Klein et al., 2000) serta memiliki makna “selalu melakukan” dan “biasa melakukan” (Oz et al., 2013).

Perilaku juga dapat didefinisikan sebagai perbuatan atau tindakan seseorang untuk merespon suatu hal dan menjadikan tindakan tersebut sebagai kebiasaan karena terdapat nilai yang diyakini (Triwibowo, 2015). Perilaku penghindaran merupakan respon universal terhadap situasi bermuatan emosional yang paling sering dikaitkan dengan kecemasan atau ketakutan. Perilaku penghindaran berupa tindakan apa pun untuk menghindari atau melarikan diri dari pikiran atau perasaan tertentu (Baker et al., 2016).

Perilaku penghindaran juga dapat didefinisikan sebagai perilaku apapun yang dilakukan dengan tujuan mengalihkan diri dari situasi yang tidak diinginkan (Sheynin et al., 2014). Berdasarkan makna-makna tersebut, perilaku penghindaran dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menghindari suatu hal. Dari definisi yang telah disebutkan, maka perilaku penghindaran kejahatan siber keuangan dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menjaga dirinya agar tidak menjadi korban kejahatan siber keuangan.

2.2 Faktor-Faktor yang Mempengaruhi Perilaku Penghindaran Kejahatan Siber Keuangan

2.2.1 Persepsi Kerentanan

Persepsi kerentanan atau *perceived susceptibility* merupakan keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik (Liang & Xue, 2010). Persepsi kerentanan adalah salah satu variabel yang digunakan untuk menilai evaluasi seseorang terkait kemungkinan mereka

terkontaminasi oleh sesuatu yang buruk atau membahayakan (Levkovich & Shinan-Altman, 2021). Persepsi kerentanan juga dapat diartikan sebagai kepercayaan seseorang dengan menganggap suatu peristiwa yang buruk adalah hasil dari melakukan perilaku tertentu. *Perceived susceptibility* atau persepsi kerentanan juga diartikan sebagai kerentanan yang dirasakan yang merujuk pada kemungkinan seseorang dapat menjadi suatu korban tindakan negatif. Persepsi kerentanan ini memiliki hubungan positif dengan perilaku yang positif. Jika kerentanan terhadap risiko tinggi maka perilaku pencegahan risiko yang dilakukan seseorang juga tinggi. Variabel tersebut dipilih karena hasil penelitian terkait variabel tersebut pada penelitian-penelitian sebelumnya masih inkonsisten.

2.2.2 Persepsi Keparahan

Persepsi keparahan adalah perasaan yang dapat mendorong individu untuk melakukan perilaku tertentu. Semakin tinggi individu percaya terhadap keparahan sebuah tindakan, maka semakin tinggi pula individu memiliki keinginan untuk melakukan sebuah perilaku untuk menghindari keparahan tersebut (Kasmaei et al., 2014). Persepsi keparahan merupakan keyakinan individu mengenai keparahan yang dirasakan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber (Liang & Xue, 2010).

2.2.3 Persepsi Ancaman

Persepsi ancaman atau *perceived threat* merupakan keyakinan individu akan menjadi korban ancaman teknologi informasi (Liang & Xue, 2009b). Persepsi

ancaman didefinisikan sebagai situasi yang sulit atau meresahkan individu (Bennett & Galpert, 1992). Persepsi ancaman juga dapat didefinisikan sebagai penilaian kognitif individu tentang kemungkinan bahaya akan mempengaruhi mereka dan seberapa buruknya jika hal itu terjadi. Menurut (Bennett & Galpert, 1992), tingkat ancaman diukur dengan satu item di mana subjek menunjukkan tingkat kekhawatiran yang disebabkan oleh peristiwa yang mengancam mereka. Semakin tinggi persepsi ancaman yang diyakini maka semakin tinggi pula tingkat perilaku penghindaran terhadap tindakan yang mengancam mereka.

2.2.4 Efikasi Diri

Efikasi diri atau *self efficacy* merupakan keyakinan individu dalam mengambil tindakan pengamanan (Liang & Xue, 2010). Efikasi diri juga dapat diartikan sebagai keyakinan yang dimiliki individu atas kemampuan yang ada didalam dirinya untuk melakukan sebuah perilaku. *Self efficacy* terdapat dalam diri seseorang saat ini, bukan dalam masa lalu atau masa depan. Menurut (Liang & Xue, 2010), efikasi diri merupakan penentu penting dari motivasi penghindaran. Kepercayaan diri individu memiliki peran sangat penting dalam perubahan perilaku. Kepercayaan diri yang dimiliki dapat menjadi motivasi untuk diri sendiri dalam melakukan perubahan untuk melakukan perilaku penghindaran kejahatan siber keuangan. Variabel ini digunakan karena kepercayaan diri individu penting dimiliki untuk meyakinkan bahwa setiap individu memiliki kekuatan untuk melakukan sesuatu perilaku penghindaran kejahatan siber keuangan.

2.2.5 Efektivitas Perlindungan

Efektivitas perlindungan didefinisikan sebagai penilaian individu dari tindakan pengamanan mengenai seberapa efektif hal itu dapat diterapkan untuk menghindari ancaman teknologi informasi yang berbahaya (Liang & Xue, 2010). Misalnya, penilaian individu mengenai seberapa efektif pendidikan *anti-phishing* dapat diterapkan untuk menghindari serangan *phishing*. Dalam penelitian ini, suatu upaya perlindungan dapat dikatakan efektif ketika upaya tersebut dapat meminimalkan kerentanan serangan kejahatan siber keuangan. Upaya yang dapat digunakan dalam perlindungan terhadap kejahatan siber keuangan adalah penggunaan *software* perlindungan seperti antivirus, anti *malware,* anti *ransomware,* dan anti *spyware.* Variabel efektivitas perlindungan digunakan dalam penelitian ini karena efektivitas suatu *software* perlindungan akan meningkatkan kepercayaan pengguna bahwa perangkat lunak tersebut akan memberikan manfaat bagi dirinya dan kemudian akan berpengaruh terhadap motivasi penggunaan perangkat lunak tersebut.

2.2.6 *Safeguard Cost*

Safeguard cost didefinisikan sebagai upaya fisik dan kognitif seperti waktu, uang, ketidaknyamanan dan pemahaman yang diperlukan dengan menggunakan tindakan pengamanan (Liang & Xue, 2009b). *Safeguard cost* juga dapat diartikan sebagai segala macam upaya yang diperlukan untuk menghindari ancaman kejahatan. Dalam hal penelitian ini, upaya yang diperlukan dalam pemasangan *software* perlindungan atas kejahatan siber keuangan. *Safeguard cost* dipilih sebagai variabel dalam penelitian ini karena hasil pengujian terkait pengaruh

safeguard cost terhadap perilaku penghindaran kejahatan siber pada penelitian-penelitian sebelumnya masih inkonsisten.

2.2.7 Antisipasi Penyesalan

Antisipasi penyesalan atau *anticipated regret* didefinisikan sebagai respon afektif negatif yang diharapkan yang akan dialami pengguna teknologi jika individu gagal mengambil tindakan perlindungan yang diperlukan terhadap ancaman teknologi informasi (Liang & Xue, 2018). *Anticipated regret* juga dapat diartikan sebagai penyesalan tindakan atau penyesalan tidak bertindak. Penyesalan tindakan mencakup penyesalan yang dihasilkan dari terlibat dalam perilaku tertentu sementara penyesalan tidak bertindak dihasilkan dari kegagalan individu untuk terlibat dalam perilaku tertentu (Brewer et al., 2016). Variabel ini dipilih untuk digunakan karena belum banyak penelitian terkait perilaku penghindaran siber keuangan yang menggunakan variabel penyesalan yang diantisipasi.

2.2.8 Motivasi Penghindaran Kejahatan Siber Keuangan

Motivasi penghindaran atau *avoidance motivation* didefinisikan sebagai seberapa termotivasi pengguna untuk menghindari ancaman teknologi informasi dengan melakukan atau menggunakan ukuran atau metode pengamanan (Liang & Xue, 2010). Motivasi penghindaran menggambarkan individu yang didorong oleh keinginan untuk menghindari masalah yang menyusahkan dan hasil yang tidak diinginkan (Braverman & Frost, 2012). Motivasi penghindaran secara tradisional terhubung dengan konsep seperti keengganan, hukuman, dan ancaman (Elliot et al., 2013). Variabel ini digunakan dalam penelitian ini karena peningkatan motivasi

penghindaran kejahatan siber akan meningkatkan suatu pola kebiasaan atau perilaku penghindaran kejahatan siber.

2.3 *Literature Review*

Tabel 2.1 Penelitian Terdahulu

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	Variabel Dependen		
1	(Verkijika, 2019)	Perilaku penghindaran serangan *phishing*	• Efikasi Diri • Gender • *Anticipated Regret*	• *Phising Avoidance Motivation and Behaviour*	• Metode Penelitian: Kuantitatif; • Sampel: 231 *device users;* • Sumber Data: Primer; • Teori: *Technology Threat Avoidance Theory;*	• *Self Efficacy* berpengaruh positif terhadap *mobile phising avoidance motivation and behaviour.* • *Anticipated Regret* berpengaruh positif terhadap *mobile phising avoidance motivation and behaviour.*
2	(Tang et al., 2021)	Perilaku penghindaran serangan *scam*	• *Governement Social Media Participation* • *Perceived Severity* • *Perceived Vulnerability* • *Sefl-efficacy* • *Response-Efficacy*	• *Information Security Behaviour*	• Metode Penelitian: Kuantitatif; • Sampel: Pengguna sosial media yang mengikuti akun pemerintah; • Sumber Data: Primer; • Teori: *Protection Motivation Theory, Cultivation Theory;* • Alat Ukur: Teknik PLS-SEM	• *GSM Participation* berpengaruh positif terhadap *Information Security Behaviour,* • *Perceived Severity* berpengaruh positif terhadap *Information Security Behaviour,* • *Perceived Vulerability* berpengaruh positif terhadap *Information Security Behaviour,*

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	Variabel Dependen		
					menggunakan SmartPLS	• *Self-efficacy* berpengaruh positif terhadap *Information Security Behaviour*, • *Response-efficacy* berpengaruh positif terhadap *Information Security Behaviour*
3	(Sylvester, 2022)	Perilaku penghindaran serangan *phishing*	• *Perceived Susceptibility* • *Perceived Severity* • *Perceived Threat of being Pished* • *Safeguard Effectiveness* • *Safeguard Cost* • *Self Efficacy* • *Avoidance Motivation*	• *Phising Avoidance Behaviour*	• Metode Penelitian: Kuantitatif; • Sampel: 137 pengguna mobile devices; • Sumber Data: Primer; • Teori: *Technology Threat Avoidance Theory;*	• *Perceived Susceptibility* dan *Perceived Severity* memiliki korelasi yang signifikan terhadap *Perceived Threat of being phished*; • Motivasi pengguna perangkat seluler untuk menghindari ancaman berkorelasi dengan perilaku pengguna dalam menghindari ancaman; • Kerentanan pengguna perangkat seluler terhadap serangan *phishing* dapat dikurangi dengan persepsi mereka tentang ancaman.
4	(Saidi & Prayudi, 2021)	Perilaku penghindaran serangan *phishing*	• *Perceived Severity* • *Perceived Susceptibility*	• Perilaku penghindaran terhadap	• Metode Penelitian: Kuantitatif dan Kualitatif;	• Terdapat keterkaitan antar faktor yang sangat berpengaruh yaitu faktor *behavioral intention* dengan

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	**Variabel Dependen**		
			• *Perceived Threat* • *Safeguard effectiveness* • *Safeguard Cost* • *Self efficacy* • *Behavioural Intention* • *Avoidance Motivation*	serangan *phising*	• Sampel: Mahasiswa, Dosen, dan Karyawan Universitas; • Sumber Data: Primer; • Teori: *Technology Threat Avoidance Theory;* • Alat Ukur: Uji MANOVA menggunakan SPSS	faktor *self-efficacy – security awareness*
5	(Mark et al., 2021)	Perilaku penghindaran serangan *phishing*	• *Perceived Severity* • *Perceived Susceptibility* • *Perceived Threat* • *Safeguard effectiveness* • *Safeguard Cost* • *Self efficacy* • *Behavioural Intention* • *Avoidance Motivation*	• *Avoidance Behavior to IT Security Threats*	• Metode Penelitian: Kuantitatif; • Sampel: 178 warga AS yang merupakan pengguna PC yang berinteraksi dalam sosial media dan berusia 18-75 tahun; • Sumber Data: Primer; • Teori: *Technology Threat Avoidance Theory;* • Alat Ukur: Uji ANOVA dan Regresi	• Interaksi antara *Perceived Susceptibility* dan *Perceived Severity* berpegaruh signifikan terhadap *Perceived Threat;* • *Perceived Threat* berpengaruh signifikan terhadap *Avoidance Motivation;* • *Safeguard Effectiveness* berpengaruh signifikan terhadap *Avoidance Motivation;* • *Self Efficacy* berpengaruh signifikan terhadap *Avoidance Motivation;*

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	Variabel Dependen		
						• *Avoidance Motivation* berpengaruh signifikan terhadap *Avoidance Behavior*
6	(Djatsa, 2020)	Perilaku kemanan pengguna *device*	• *Perceived Threat*	• *User's Online Security Behavior* • *Users's Avoidance Motivation*	• Metode Penelitian: Kuantitatif; • Sampel: 109 peserta yang dipilih secara acak di AS; • Sumber Data: Primer; • Alat Ukur: Uji korelasi spearman	• Tidak terdapat korelasi antara *Perceived Threat* dengan *User's Online Security Avoidance*; • Tidak terdapat korelasi antara *Perceived Threat* dengan *User's Avoidance Motivation*
7	(Butler, 2020)	Perilaku penghindaran serangan kejahatan siber	-	-	• Metode Penelitian: Kualitatif; • Sampel: 27 Literatur; • Sumber Data: Sekunder	• Terdapat enam faktor yang berpengaruh terhadap *Threat Avoidance Behavior* yaitu: pengetahuan dan kesadaran, kesalahpahaman dan kepercayaan, perhitungan biaya dan manfaat, kecerobohan, kefektifan yang dirasakan, serta keterampilan dan kepuasan yang dirasakan pengguna.
8	(Bax et al., 2021)	Perilaku penghindaran serangan *phishing*	• *Perceived Severity*	• *Protection Behaviour*	• Metode Penelitian: Kuantitatif;	• *Reward* beroengaruh terhadap *maladaptive behaviour;*

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	**Variabel Dependen**		
			• *Perceived Vulnerability* • *Fear* • *Response Efficacy* • *Self-Efficacy* • *Reward* • *Response Cost* • *Protection Motivation*		• Sampel: 650 pengguna internet yang berpotensi menerima email *phising*; • Sumber Data: Primer; • Teori: *Protection Motivation Theory;* • Alat Ukur: Uji Validitas, Reliabilitas	• *Reward* tidak berpengaruh terhadap *protection behaviour* dalam menghadapi ancaman *phishing;* • *Response Cost* berpengaruh terhadap *Maladaptive Behaviour* • *Response Cost* berpengaruh terhadap *Protection Behaviour*
9	(Gillam & Foster, 2020)	Perilaku keamanan siber	• *Perceived Severity* • *Perceived Susceptibility* • *Perceived effectiveness* • *Perceived Cost* • *Self Efficacy*	• *Avoidance Behaviour*	• Metode Penelitian: Kuantitatif; • Sampel: 184 orang dewasa yag bekerja di Amerika Serikat; • Sumber Data: Primer; • Teori: Technology Threat Avoidance Theory; • Alat Ukur: SPSS	• *Perceived Susceptibiliy* berpengaruh terhadap *Avoidance Behaviour;* • *Perceived Cost* berpengaruh terhadap *Avoidance Behaviour;* • *Self Efficacy* berpengaruh terhadap *Avoidance Behaviour*
10	(Arachchilage et al., 2016; Baral et al., n.d.)	Perilaku penghindaran serangan *phishing*	• *Threat Perception* • *Safeguard Eeffectiveness* • *Self Efficacy*	• *Phising Avoidance Behaviour*	• Metode Penelitian: Kuantitatif; • Sampel: 20 mahasiswa tahun ketiga jurusan Ilmu	• *Threat Perception* berpengaruh positif terhadap *Phishing Avoidance Behaviour;*

No	Peneliti dan Tahun	Ruang Lingkup Penelitian	Variabel Penelitian		Metode, Sampel, dan Alat Analisis	Hasil Penelitian
			Variabel Independen	Variabel Dependen		
			• *Perceived Susceptibility* • *Perceived Severity* • *Safeguard Cost*		Komputer dari Brunel University, UK; • Sumber Data: Primer; • Teori: *Technology Threat Avoidance Theory*	• *Safeguard Effectiveness* berpengaruh positif terhadap *Phishing Avoidance Behaviour;* • *Self-Efficaccy* berpengaruh positif terhadap *Phishing Avoidance Behaviour;* • *Perceived Susceptibility* berpengaruh positif terhadap *Phishing Avoidance Behaviour;* • *Perceived Severity* berpengaruh positif terhadap *Phishing Avoidance Behaviour;* • *Safeguardcost* berpengaruh negatif terhadap *Phishing Avoidance Behaviour*

2.4 Perumusan Hipotesis

2.4.1 Pengaruh Persepsi Kerentanan Terhadap Persepsi Ancaman

Persepsi kerentanan atau *perceived susceptibility* adalah salah satu variabel yang digunakan untuk menilai evaluasi seseorang terkait kemungkinan mereka terkontaminasi oleh sesuatu yang buruk atau membahayakan (Levkovich & Shinan-Altman, 2021). *Perceived susceptibility* juga dapat diartikan sebagai kepercayaan seseorang dengan menganggap suatu peristiwa yang buruk adalah hasil dari melakukan perilaku tertentu. Persepsi kerentanan juga diartikan kerentanan yang dirasakan yang merujuk pada kemungkinan seseorang dapat menjadi suatu korban tindakan negatif. Dalam *Technology Threat Avoidance Theory*, persepsi kerentanan diartikan sebagai keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik (Liang & Xue, 2010).

Banyaknya tindakan kejahatan siber yang terjadi pada era digital ini dapat menyebabkan para pengguna teknologi merasa rentan untuk menjadi korban kejahatan siber. Persepsi kerantanan dapat berpengaruh terhadap persepsi ancaman karena ketika pengguna teknologi merasa rentan, maka mereka akan meyakini bahwa terdapat kejahatan siber yang mengancam keamanan siber mereka. Dalam penelitian yang dilakukan oleh (Arachchilage et al., 2016); (Gillam & Foster, 2020); (Mark et al., 2021); (Saidi & Prayudi, 2021); dan (Sylvester, 2022) menunjukkan bahwa persepsi kerentanan berpengaruh positif terhadap persepsi ancaman.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H1: Persepsi kerentanan berpengaruh positif terhadap persepsi ancaman

2.4.2 Pengaruh Persepsi Keparahan Terhadap Persepsi Ancaman

Secara umum persepsi keparahan adalah perasaan yang dapat mendorong individu untuk melakukan perilaku tertentu. Semakin tinggi individu percaya terhadap keparahan sebuah tindakan, maka semakin tinggi pula individu memiliki keinginan untuk melakukan sebuah perilaku untuk menghindari keparahan tersebut (Kasmaei et al., 2014). Dalam TTAT, dijelaskan bahwa persepsi keparahan merupakan keyakinan individu mengenai keparahan yang dirasakan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber (Liang & Xue, 2010).

Dalam konteks penghindaran kejahatan siber, ketika pengguna teknologi informasi meyakini bahwa kejahatan siber akan menciptakan suatu kondisi yang parah maka mereka akan meyakini pula bahwa kejahatan siber keuangan merupakan ancaman yang serius. Penelitian yang dilakukan oleh (Arachchilage et al., 2016); (Mark et al., 2021); (Saidi & Prayudi, 2021); dan (Sylvester, 2022) membuktikan bahwa persepsi keparahan berpengaruh positif terhadap persepsi ancaman, sedangkan penelitian oleh (Gillam & Foster, 2020) menunjukkan bahwa persepsi keparahan tidak berpengaruh terhadap persepsi ancaman. Hal tersebut menunjukkan bahwa hasil penelitian terkait pengaruh persepsi keparahan terhadap persepsi ancaman masih inkonsisten.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H2: Persepsi keparahan berpengaruh positif terhadap persepsi ancaman.

2.4.3 Pengaruh Interaksi Persepsi Kerentanan dan Persepsi Keparahan Terhadap Persepsi Ancaman

Persepsi kerentanan atau *perceived susceptibility* merupakan keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik (Liang & Xue, 2009b). Persepsi keparahan atau *perceived severity* merupakan keyakinan individu mengenai keparahan yang dirasakan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber (Liang & Xue, 2009b).

Konsisten dengan TTAT (Liang & Xue, 2009b), perilaku penghindaran ancaman pengguna teknologi informasi ditentukan oleh motivasi penghindaran, yang pada gilirannya, dipengaruhi oleh persepsi ancaman yang diyakini. Persepsi ancaman dipengaruhi oleh persepsi keparahan dan persepsi kerentanan. Persepsi ancaman juga dipengaruhi oleh interaksi antara persepsi keparahan dan persepsi kerentanan. Ketika seseorang merasa rentan untuk menjadi korban serangan siber keuangan maka ia juga akan meyakini bahwa keparahan akan menimpa dirinya, begitu pula sebaliknya. Ketika seseorang mempercayai persepsi kerentanan dan persepsi keparahan tersebut secara bersamaan, maka ia akan merasa terancam untuk menjadi korban serangan siber keuangan. Dalam penelitian yang dilakukan oleh

(Mark et al., 2021) dan (Sylvester, 2022), persepsi kerentanan dan persepsi keparahan memiliki pengaruh yang signifikan terhadap persepsi ancaman.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H3: Interaksi antara persepsi kerentanan dan persepsi memiliki pengaruh positif terhadap persepsi ancaman.

2.4.4 Pengaruh Persepsi Ancaman Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Persepsi ancaman didefinisikan sebagai situasi yang sulit atau meresahkan individu (Bennett & Galpert, 1992). Persepsi ancaman juga dapat didefinisikan sebagai penilaian kognitif individu tentang kemungkinan bahaya akan mempengaruhi mereka dan seberapa buruknya jika hal itu terjadi. Menurut (Bennett & Galpert, 1992), tingkat ancaman diukur dengan satu item di mana subjek menunjukkan tingkat kekhawatiran yang disebabkan oleh peristiwa yang mengancam mereka. Dalam teori TTAT, persepsi ancaman atau *perceived threat* diartikan sebagai keyakinan individu akan menjadi korban ancaman teknologi informasi (Liang & Xue, 2009b).

Dalam kaitannya dengan motivasi penghindaran kejahatan siber keuangan, ketika seseorang merasa dirinya terancam untuk menjadi korban serangan kejahatan siber keuangan maka ia akan termotivasi untuk menghindari ancaman tersebut. Dalam penelitian yang dilakukan oleh (Mark et al., 2021) menunjukkan bahwa faktor persepsi ancaman memiliki pengaruh positif terhadap motivasi penghindaran ancaman *phishing* sedangkan dalam penelitian oleh (Djatsa, 2020) menunjukkan

bahwa *perceived threat* tidak berpengaruh terhadap motivasi penghindaran kejahatan siber. Hal tersebut menunjukkan bahwa penelitian terkait pengaruh *perceived threat* terhadap motivasi penghindaran ancaman kejahatan siber masih inkonsisten.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H4: Persepsi ancaman berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan.

2.4.5 Pengaruh Efikasi Diri Terhadap Motivasi Penghindaran Terhadap Kejahatan Siber Keuangan

Efikasi diri atau *self efficacy* merupakan keyakinan individu dalam mengambil tindakan pengamanan (Liang & Xue, 2010). Efikasi diri merupakan penentu penting dari motivasi penghindaran. *Self efficacy* terdapat dalam diri seseorang saat ini, bukan dalam masa lalu atau masa depan. Menurut (Liang & Xue, 2010), efikasi diri merupakan penentu penting dari motivasi penghindaran. Kepercayaan diri individu memiliki peran sangat penting dalam perubahan perilaku.

Mengacu pada TTAT, kaitan efikasi diri dengan perilaku penghindaran kejahatan siber keuangan yaitu kepercayaan diri yang dimiliki dapat menjadi motivasi untuk diri sendiri dalam melakukan perubahan untuk melakukan perilaku penghindaran terhadap hal-hal yang tidak diinginkan. Penelitian sebelumnya oleh (Gillam & Foster, 2020); (Butler, 2020); (Mark et al., 2021); (Saidi & Prayudi, 2021); (Tang et al., 2021); dan (Verkijika, 2019) telah mengungkapkan bahwa

individu lebih termotivasi untuk melakukan perilaku terkait keamanan TI karena tingkat efikasi diri mereka meningkat.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H5: Efikasi diri berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan

2.4.6 Pengaruh Efektivitas Perlindungan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Efektivitas perlindungan didefinisikan sebagai penilaian individu dari tindakan pengamanan mengenai seberapa efektif hal itu dapat diterapkan untuk menghindari ancaman TI yang berbahaya (Liang & Xue, 2010). Misalnya, penilaian individu mengenai seberapa efektif pendidikan *anti-phishing* dapat diterapkan untuk menghindari serangan *phishing*. Dalam penelitian ini, suatu upaya perlindungan dapat dikatakan efektif ketika upaya tersebut dapat meminimalkan kerentanan serangan kejahatan siber keuangan. Upaya yang dapat digunakan dalam perlindungan terhadap kejahatan siber keuangan adalah penggunaan *software* perlindungan seperti antivirus, *anti malware, anti ransomware,* dan *anti spyware*. Dalam penelitian yang dilakukan oleh Butler (2020) dan Arachchilage, *et al.*, (2016) membuktikan bahwa efektivitas perlindungan berpengaruh terhadap motivasi penghindaran kejahatan siber.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H6: Efektivitas perlindungan berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan

2.4.7 Pengaruh *Safeguard Cost* Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Safeguard cost didefinisikan sebagai upaya fisik dan kognitif seperti waktu, uang, ketidaknyamanan dan pemahaman yang diperlukan dengan menggunakan tindakan pengamanan (Liang & Xue, 2009b). *Safeguard cost* juga dapat diartikan sebagai segala macam upaya yang diperlukan untuk menghindari ancaman kejahatan. Dalam hal penelitian ini, upaya yang dilakukan berupa pemasangan *software* perlindungan atas kejahatan siber keuangan.

Dalam penelitian yang dilakukan oleh (Butler, 2020) menunjukkan bahwa perhitungan biaya berpengaruh terhadap perilaku penghindaran. Hal tersebut sejalan dengan hasil penelitian oleh (Gillam & Foster, 2020) yang menunjukkan bahwa *perceived cost* berpengaruh terhadap perilaku penghindaran. Sedangkan penelitian yang dilakukan oleh (Arachchilage et al., 2016) membuktikan bahwa *safeguard cost* tidak berpengaruh terhadap motivasi penghindaran. Hal tersebut menunjukkan bahwa penelitian terkait pengaruh *safeguard cost* terhadap motivasi penghindaran belum konsisten.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H7: *Safeguard cost* berpengaruh negatif terhadap motivasi penghindaran kejahatan siber keuangan

2.4.8 Pengaruh Antisipasi Penyesalan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Dalam *regret theory*, antisipasi penyesalan didefinisikan sebagai reaksi seseorang untuk mengantisipasi penyesalan sebelum membuat keputusan (Loomes & Sugden, 1982); (Bell, 1982); (Fishburn, 1982)). Antisipasi pennyesalan adalah reaksi emosional negatif yang dialami individu sebagai hasil dari membandingkan hasil yang diantisipasi dari keputusan mereka untuk tidak bertindak dengan hasil yang akan mereka alami jika mereka bertindak (Xiling et al., 2018). *Anticipated regret* juga dapat diartikan sebagai penyesalan tindakan atau penyesalan tidak bertindak. Penyesalan tindakan mencakup penyesalan yang dihasilkan dari terlibat dalam perilaku tertentu sementara penyesalan tidak bertindak dihasilkan dari kegagalan individu untuk terlibat dalam perilaku tertentu (Brewer et al., 2016).

Mengacu pada penghindaran kejahatan siber, penyesalan yang diantisipasi atau *anticipated regret* didefinisikan sebagai respon afektif negatif yang diharapkan yang akan dialami pengguna teknologi jika individu gagal mengambil tindakan perlindungan yang diperlukan terhadap ancaman teknologi informasi (Liang & Xue, 2018). Kaitannya dengan motivasi penghindaran kejahatan siber keuangan yaitu ketika seseorang dihadapkan dengan ancaman kejahatan siber keuangan, maka akan menyebabkan penyesalan ketika ia gagal mengambil keputusan untuk melindungi diri dari ancaman kejahatan siber keuangan. Dalam penelitian ini, fokusnya adalah penyesalan kelambanan pengambilan keputusan untuk menghindari serangan siber keuangan. Hal ini karena ketika menghadapi ancaman,

hasil negatif yang mengarah pada penyesalan cenderung lebih besar jika seseorang gagal mengambil keputusan.

Penelitian sebelumnya yang dilakukan oleh (Verkijika, 2019) telah membuktikan bahwa *anticipated regret* berpengaruh positif terhadap *avoidance motivation*. Namun, penelitian serupa yang menggunakan variabel ini masih terbatas, sehingga perlu dilakukan penelitian lebih lanjut pada objek yang berbeda.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H8: Antisipasi penyesalan berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan.

2.4.9 Pengaruh Motivasi Penghindaran Kejahatan Siber Keuangan Terhadap Perilaku Penghindaran Kejahatan Siber Keuangan

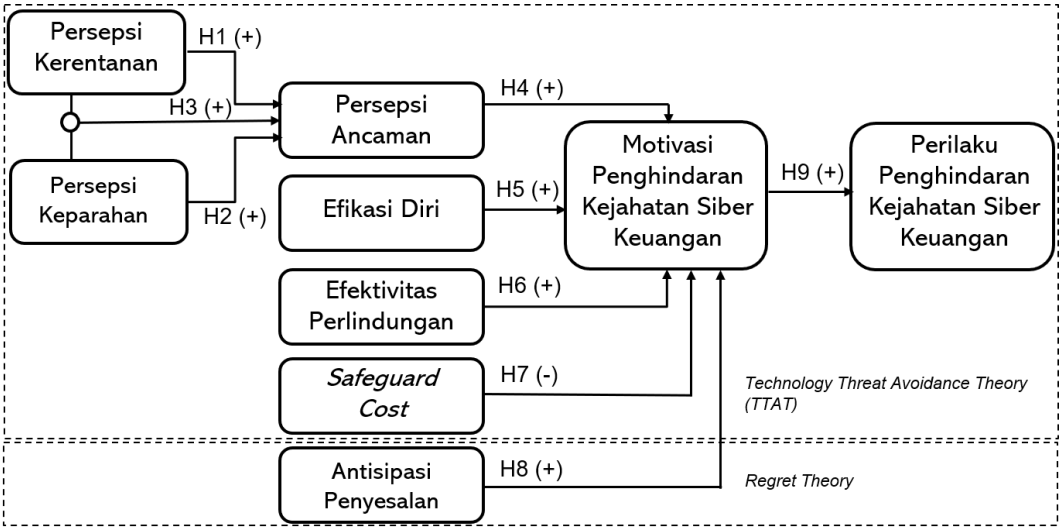
Motivasi penghindaran atau *avoidance motivation* didefinisikan sebagai seberapa termotivasi pengguna untuk menghindari ancaman teknologi informasi dengan melakukan atau menggunakan ukuran atau metode pengamanan (Liang & Xue, 2010). Motivasi penghindaran menggambarkan individu yang didorong oleh keinginan untuk menghindari masalah yang menyusahkan dan hasil yang tidak diinginkan (Braverman & Frost, 2012). Motivasi penghindaran secara tradisional terhubung dengan konsep seperti keengganan, hukuman, dan ancaman (Elliot et al., 2013). Dalam penelitian yang dilakukan oleh (Gillam & Foster, 2020); (Butler, 2020); (Mark et al., 2021); (Arachchilage et al., 2016) dan (Verkijika, 2019) membuktikan bahwa motivasi penghindaran berpengaruh positif terhadap perilaku penghindaran kejahatan siber.

Berdasarkan pembahasan di atas, maka dirumuskan hipotesis sebagai berikut:

H9: Motivasi penghindaran kejahatan siber keuangan berpengaruh positif terhadap perilaku penghindaran kejahatan siber keuangan.

2.5 Kerangka Model Penelitian

Berdasarkan hipotesis yang telah dikembangkan, berikut ini kerangka model penelitian yang dirumuskan:



Gambar 2.1 Kerangka Model Penelitian

BAB 3

METODOLOGI PENELITIAN

3.1 Populasi dan Sampel

Populasi adalah kumpulan individu atau objek yang diketahui memiliki kesamaan karakteristik (Schindler, 2019). Populasi dalam penelitian ini adalah pekerja yang bekerja pada sektor keuangan di wilayah Indonesia. Sedangkan sampel penelitian ini adalah pekerja sektor keuangan di Indonesia yang menggunakan perangkat elektronik dalam bekerja. Sampel tersebut dipilih karena industri sektor keuangan termasuk menjadi sektor terbesar yang menjadi sasaran kejahatan siber. Selain itu, dengan menyediakan layanan keuangan, dapat diasumsikan bahwa seharusnya pekerja sektor keuangan lebih peduli dengan keamanan ruang siber dan telah memperoleh pelatihan dengan intensitas lebih sering dibandingkan dengan masyarakat umum. Dengan menyelidiki perilaku penghindaran kejahatan siber keuangan oleh pekerja sektor keuangan terlebih dahulu, dapat membantu mencegah, mendeteksi, dan mengurangi risiko kejahatan siber dalam sistem keuangan secara keseluruhan. Sedangkan untuk pengambilan sampel, peneliti menggunakan teknik *convenience sampling*. Teknik *convenience sampling* merupakan teknik pemilihan sampel yang digunakan ketika peneliti tidak memiliki data terkait populasi dalam bentuk *sampling frame* dan peneliti kemudian memilih sampel berdasarkan prinsip kemudahan dalam mengambil atau memilih sampel (Abdillah & Jogiyanto, 2015). Teknik tersebut dipilih karena peneliti tidak mengetahui secara pasti terkait jumlah populasi yang digunakan.

3.2 Jenis dan Sumber Data

Sumber data dalam penelitian ini berupa data primer yang diperoleh langsung dari responden. Data primer merupakan data yang belum pernah digunakan dan diolah oleh suatu pihak untuk kepentingan tertentu sehingga data tersebut menunjukkan keaslian informasi yang terkandung di dalam data tersebut (Abdillah & Jogiyanto, 2015). Metode pengumpulan data dilakukan dengan menggunakan kuesioner *offline (paper-based)* dan kuesioner *online*. Kuesioner merupakan suatu metode pengumpulan data primer dengan menggunakan sejumlah item pertanyaan dalam format tertentu (Abdillah & Jogiyanto, 2015). Dalam penelitian ini, peneliti menggunakan kuesioner dengan model kuesioner tertutup. Variabel dalam penelitian ini adalah perilaku penghindaran kejahatan siber keuangan sebagai variabel dependen; persepsi kerentanan, persepsi keparahan, persepsi ancaman, efikasi diri, efektivitas perlindungan, *safeguard cost*, dan antisipasi penyesalan sebagai serta motivasi penghindaran kejahatan siber keuangan sebagai variabel independen.

3.3 Teknik Pengambilan Sampel

Teknik pengambilan sampel dalam penelitian ini adalah menggunakan teknik *convenience sampling*. Teknik *convenience sampling* merupakan teknik pemilihan sampel yang digunakan ketika peneliti tidak memiliki data terkait populasi dalam bentuk *sampling frame* dan peneliti kemudian memilih sampel berdasarkan prinsip kemudahan dalam mengambil atau memilih sampel (Abdillah & Jogiyanto, 2015). Teknik tersebut dipilih karena peneliti tidak mengetahui secara pasti terkait jumlah populasi yang digunakan.

Penentuan jumlah sampel dalam penelitian ini menggunakan rumus Hair karena jumlah populasi belum diketahui secara pasti. Menurut (Hair et al., 2019), jumlah sampel yang representatif tergantung pada jumlah indikator dikali 5 (lima) sampai dengan 10 (sepuluh). Sehingga perhitungan sampel minimal untuk penelitian ini adalah sebagai berikut:

Jumlah sampel = Jumlah indikator x 5

= 34 x 5

= 170

Data dalam penelitian ini diukur dengan menggunakan *likert* dengan skala 6 poin untuk menghindari jawaban netral oleh responden. Skala tersebut memiliki nilai 6 poin untuk jawaban sangat setuju, 5 poin untuk jawaban setuju, 4 poin untuk jawaban agak setuju, 3 poin untuk jawaban agak tidak setuju, 2 poin untuk jawaban tidak setuju, dan 1 poin untuk jawaban sangat tidak setuju.

3.4 Definisi Operasional Variabel Penelitian

Variabel merupakan suatu karakteristik, sifat, atau atribut yang diukur atau simbol yang diberi nilai. Variabel terdiri dari beberapa jenis yaitu variabel independen, variabel dependen, variabel moderasi, variabel intervening, variabel control, dan variabel asing (Schindler, 2019). Dalam penelitian ini terdapat tiga macam variabel yang digunakan, yaitu variabel independen, variabel intervening, dan variabel dependen.

Variabel independen atau variabel bebas merupakan variabel yang dimanipulasi, sehingga menimbulkan pengaruh atau perubahan pada variabel dependen atau variabel terikat. Sedangkan variabel intervening merupakan faktor

yang mempengaruhi fenomena yang diamati tetapi tidak dapat dilihat, diukur, atau dimanipulasi; dengan demikian, efeknya harus disimpulkan dari efek variabel independen dan moderasi pada variabel dependen. Di sisi lain, variabel dependen merupakan variabel yang diukur, diprediksi, atau dipantau dan diharapkan dipengaruhi oleh manipulasi variabel independent (Schindler, 2019).

Penelitian ini memiliki 8 variabel independen yaitu, persepsi kerentanan, persepsi keparahan, persepsi ancaman, efikasi diri, efektivitas perlindungan, *safeguard cost*, antisipasi penyesalan, dan motivasi penghindaran kejahatan siber keuangan. Sedangkan untuk variabel dependen dalam penelitian ini adalah perilaku penghindaran kejahatan siber keuangan.

3.4.1 Persepsi Kerentanan

Persepsi kerentanan diartikan sebagai keyakinan individu mengenai kerentanan dirinya atas risiko menjadi korban serangan siber sehingga akan mendorong mereka untuk melakukan perilaku yang lebih baik (Liang & Xue, 2010). Banyaknya tindakan kejahatan siber yang terjadi pada era digital ini dapat menyebabkan para pengguna teknologi merasa rentan untuk menjadi korban kejahatan siber. Ketika pengguna teknologi merasa rentan, maka mereka akan meyakini bahwa terdapat kejahatan siber yang mengancam keamanan siber mereka. Kerentanan dalam hal ini dinilai dengan menggunakan indikator kemungkinan seseorang menjadi korban serangan kejahatan siber.

Berdasarkan pembahasan di atas, maka diajukan 3 pertanyaan untuk mengetahui pengaruh persepsi kerentanan terhadap persepsi ancaman dalam hal

penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009b). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.1.

Tabel 3.1 Indikator Persepsi Kerentanan

Variabel	Item Pertanyaan	Referensi
Persepsi Kerentanan	1. Sangat mungkin bagi perangkat elektronik saya untuk menjadi target kejahatan siber keuangan di masa yang akan datang. 2. Peluang saya untuk menjadi korban kejahatan siber keuangan melalui perangkat elektronik cukup besar. 3. Terdapat kemungkinan besar bahwa perangkat elektronik saya berisi atau terinfeksi *malware* (virus) yang dapat mencuri data pribadi saya.	(Liang & Xue, 2009b), dengan modifikasi

3.4.2 Persepsi Keparahan

Persepsi keparahan atau *perceived severity* merupakan keyakinan individu mengenai keparahan yang dirasakan apabila menjadi korban serangan siber yang didasarkan pada informasi atau pengetahuan yang dimiliki atau kepercayaan individu terhadap adanya risiko terserang kejahatan siber (Liang & Xue, 2010). Secara umum persepsi keparahan adalah perasaan yang dapat mendorong individu untuk melakukan perilaku tertentu. Semakin tinggi individu percaya terhadap keparahan sebuah tindakan, maka semakin tinggi pula individu memiliki keinginan untuk melakukan sebuah perilaku untuk menghindari keparahan tersebut (Kasmaei et al., 2014). Persepsi keparahan diukur dengan menggunakan indikator terkait dengan akibat yang diterima oleh pengguna komputer ketika menjadi korban serangan siber keuangan.

Berdasarkan pembahasan di atas, maka diajukan 4 pertanyaan untuk mengetahui pengaruh persepsi keparahan terhadap persepsi ancaman dalam hal

penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009b). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.2.

Tabel 3.2 Indikator Persepsi Keparahan

Variabel	Item Pertanyaan	Referensi
Persepsi Keparahan	1. Pelaku kejahatan siber keuangan dapat mengumpulkan data pribadi dari perangkat elektronik milik saya tanpa sepengetahuan saya. 2. Data pribadi saya yang dikumpulkan oleh pelaku kejahatan siber keuangan dari perangkat elektronik milik saya dapat disalahgunakan. 3. Serangan kejahatan siber keuangan dapat memeperlambat kinerja perangkat elektronik dan koneksi jaringan internet saya.	(Liang & Xue, 2009b), dengan modifikasi

3.4.3 Persepsi Ancaman

Persepsi ancaman atau *perceived threat* merupakan keyakinan individu akan menjadi korban ancaman teknologi informasi (Liang & Xue, 2009b). Persepsi ancaman didefinisikan sebagai situasi yang sulit atau meresahkan individu (Bennett & Galpert, 1992). Persepsi ancaman juga dapat didefinisikan sebagai penilaian kognitif individu tentang kemungkinan bahaya akan mempengaruhi mereka dan seberapa buruknya jika hal itu terjadi. Menurut (Bennett & Galpert, 1992), tingkat ancaman diukur dengan satu item di mana subjek menunjukkan tingkat kekhawatiran yang disebabkan oleh peristiwa yang mengancam mereka.

Berdasarkan pembahasan di atas, maka diajukan 4 pertanyaan untuk mengetahui pengaruh persepsi ancaman terhadap motivasi penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009a). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.3.

Tabel 3.3 Indikator Persepsi Ancaman

Variabel	Item Pertanyaan	Referensi
Persepsi Ancaman	1. Serangan kejahatan siber keuangan pada perangkat elektronik dapat menimbulkan ancaman bagi saya. 2. Masalah yang disebabkkan oleh serangan kejahatan siber keuangan pada perangkat elektronik berbahaya bagi saya. 3. Kejahatan siber keuangan berbahaya bagi perangkat elektronik dan jaringan internet saya. 4. Saya tidak dapat membayangkan apabila saya menjadi korban kejahatan siber keuangan yang menyerang perangkat elektronik milik saya.	(Liang & Xue, 2009b), dengan modifikasi

3.4.4 Efikasi Diri

Efikasi diri atau *self efficacy* merupakan keyakinan individu dalam mengambil tindakan pengamanan (Liang & Xue, 2010). Efikasi diri merupakan penentu penting dari motivasi penghindaran. *Self efficacy* terdapat dalam diri seseorang saat ini, bukan dalam masa lalu atau masa depan. Menurut(Liang & Xue, 2010), efikasi diri merupakan penentu penting dari motivasi penghindaran. Kepercayaan diri individu memiliki peran sangat penting dalam perubahan perilaku. Kepercayaan diri yang dimiliki dapat menjadi motivasi untuk diri sendiri dalam melakukan perubahan untuk melakukan perilaku penghindaran terhadap hal-hal yang tidak diinginkan. Kaitan efikasi diri dengan perilaku penghindaran kejahatan siber keuangan yaitu semakin tinggi efikasi diri maka akan semakin tinggi pula motivasi seseorang untuk melakukan penghindaran kejahatan siber keuangan.

Berdasarkan pembahasan di atas, maka diajukan 4 pertanyaan untuk mengetahui pengaruh efikasi diri terhadap motivasi penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009a) serta (Verkijika, 2019). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.4.

Tabel 3.4 Indikator Efikasi Diri

Variabel	Item Pertanyaan	Referensi
Efikasi Diri	1. Saya yakin bahwa tanpa bantuan orang lain, saya dapat memperoleh pengetahuan terkait ancaman kejahatan siber keuangan yang dapat menyerang perangkat elektronik saya. 2. Saya merasa yakin dengan kemampuan saya untuk mendeteksi serangan kejahatan siber keuangan di perangkat elektronik saya. 3. Saya merasa yakin dengan kemampuan saya untuk mendeteksi aplikasi/*software* pada perangkat elektronik saya yang bukan berasal dari sumber terpercaya. 4. Saya yakin saya memiliki kemampuan untuk mengidentifikasi SMS/email yang mengandung tautan/*link* berbahaya pada perangkat elektronik saya.	(Liang & Xue, 2009a) dan (Verkijika, 2019), dengan modifikasi

3.4.5 Efektivitas Perlindungan

Efektivitas perlindungan didefinisikan sebagai penilaian individu dari tindakan pengamanan mengenai seberapa efektif hal itu dapat diterapkan untuk menghindari ancaman TI yang berbahaya (Liang & Xue, 2010). Misalnya, penilaian individu mengenai seberapa efektif pendidikan *anti-phishing* dapat diterapkan untuk menghindari serangan *phishing*. Dalam penelitian ini, suatu upaya perlindungan dapat dikatakan efektif ketika upaya tersebut dapat meminimalkan kerentanan serangan kejahatan siber keuangan. Upaya yang dapat digunakan dalam

perlindungan terhadap kejahatan siber keuangan adalah penggunaan *software* perlindungan seperti antivirus, *anti malware, anti ransomware,* dan *anti spyware.* Konstruk ini dinilai dengan mengajukan pertanyaan terkait manfaat yang diperoleh oleh pengguna komputer ketika menggunakan sistem perlindungan pada komputernya.

Berdasarkan pembahasan di atas, maka diajukan 4 pertanyaan untuk mengetahui pengaruh efektivitas perlindungan terhadap motivasi penghindaran kejahatan siber keuangan yang dikembangkan oleh Liang dan Xue (2009). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.5.

Tabel 3.5 Indikator Efektivitas Perlindungan

Variabel	Item Pertanyaan	Referensi
Efektivitas Perlindungan	1. *Software* perlindungan (antivirus) akan berguna untuk mendeteksi dan menghapus serangan kejahatan siber keuangan pada perangkat elektronik saya. 2. *Software* perlindungan (antivirus) dapat meningkatkan kinerja saya untuk melindungi perangkat elektronik saya dari serangan kejahatan siber keuangan. 3. *Software* perlindungan (antivirus) dapat meningkatkan efektivitas saya dalam menemukan dan menghapus serangan kejahatan siber keuangan di perangkat elektronik saya.	(Liang dan Xue, 2009), dengan modifikasi

3.4.6 *Safeguard Cost*

Safeguard cost didefinisikan sebagai upaya fisik dan kognitif seperti waktu, uang, ketidaknyamanan dan pemahaman yang diperlukan dengan menggunakan tindakan pengamanan (Liang & Xue, 2009). *Safeguard cost* juga dapat diartikan sebagai segala macam upaya yang dilakukan untuk menghindari ancaman kejahatan. Dalam penelitian ini, konstruk *safeguard cost* dinilai dengan item

pertanyaan terkait upaya yang dilakukan untuk pemasangan *software* perlindungan atas kejahatan siber keuangan.

Berdasarkan pembahasan di atas, maka diajukan 4 pertanyaan untuk mengetahui pengaruh *safeguard cost* terhadap motivasi penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009b). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.5.

Tabel 3.6 Indikator *Safeguard Cost*

Variabel	Item Pertanyaan	Referensi
Safeguard Cost	1. Proses untuk memperoleh *software* perlindungan (antivirus) pada perangkat elektronik akan membutuhkan banyak waktu & tenaga, karena proses untuk memperoleh *software* tersebut tidak mudah. 2. Proses instalasi *software* perlindungan (antivirus) pada perangkat elektronik akan membutuhkan banyak waktu & tenaga, karena proses instalasi *software* tersebut tidak mudah. 3. Adanya *software* perlindungan (antivirus) pada perangkat elektronik akan mengganggu kenyamanan saya karena *software* tersebut dapat menimbulkan masalah pada perangkat elektronik saya. 4. Berlangganan *software* perlindungan (ativirus) pada perangkat elektronik merupakan salah satu wujud pemborosan karena biaya berlangganan *software* tersebut tidak murah.	(Liang & Xue, 2009b), dengan modifikasi

3.4.7 Antisipasi Penyesalan

Antisipasi penyesalan didefinisikan sebagai respon afektif negatif yang diharapkan yang akan dialami pengguna teknologi jika individu gagal mengambil tindakan perlindungan yang diperlukan terhadap ancaman teknologi informasi (Liang & Xue, 2018). Antisipasi penyesalan juga dapat diartikan sebagai penyesalan tindakan atau penyesalan tidak bertindak. Penyesalan tindakan

mencakup penyesalan yang dihasilkan dari terlibat dalam perilaku tertentu sementara penyesalan tidak bertindak dihasilkan dari kegagalan individu untuk terlibat dalam perilaku tertentu (Brewer et al., 2016). Dalam penelitian ini, fokusnya adalah penyesalan kelambanan pengambilan keputusan untuk menghindari serangan siber keuangan. Konstruk ini dinilai dengan mengajukan pertanyaan terkait dengan perasaan yang dirasakan oleh pengguna komputer ketika hendak mengambil tindakan yang berkaitan dengan kemanan sistem.

Berdasarkan pembahasan di atas, maka diajukan 3 pertanyaan untuk mengetahui pengaruh penyesalan yang diantisipasi terhadap motivasi penghindaran kejahatan siber keuangan yang dikembangkan oleh (Verkijika, 2019). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.6.

Tabel 3.7 Indikator Antisipasi Penyesalan

Variabel	Item Pertanyaan	Referensi
Antisipasi Penyesalan	1. Saya akan menyesal apabila gagal mengambil langkah yang diperlukan untuk melindungi perangkat elektronik saya dari serangan kejahatan siber keuangan. 2. Saya akan menyesal apabila saya memasang *software* yang berasal dari sumber tidak terpercaya pada perangkat elektronik saya. 3. Saya akan menyesal apabila saya membuka tautan dari SMS/e-mail yang mengandung virus di perangkat elektronik saya.	(Verkijika, 2019)

3.4.8 Motivasi Penghindaran

Motivasi penghindaran atau *avoidance motivati*on didefinisikan sebagai seberapa termotivasi pengguna untuk menghindari ancaman teknologi informasi dengan melakukan atau menggunakan ukuran atau metode pengamanan (Liang & Xue, 2010). Motivasi penghindaran menggambarkan individu yang didorong oleh

keinginan untuk menghindari masalah yang menyusahkan dan hasil yang tidak diinginkan (Braverman & Frost, 2012).

Berdasarkan pembahasan di atas, maka diajukan 3 pertanyaan untuk mengetahui pengaruh motivasi penghindaran kejahatan siber keuangan terhadap perilaku penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009a). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.7.

Tabel 3.8 Indikator Motivasi Penghindaran Kejahatan Siber Keuangan

Variabel	Item Pertanyaan	Referensi
Motivasi Penghindaran Kejahatan Siber Keuangan	1. Saya termotivasi memperoleh pengetahuan terkait kejahatan siber keuangan untuk menghindari kejahatan siber keuangan yang menyerang perangkat elektronik milik saya. 2. Saya termotivasi menggunakan *software* perlindungan (antivirus) untuk menghindari serangan kejahatan siber keuangan pada perangkat elektronik milik saya. 3. Saya termotivasi untuk berbagi pengetahuan terkait kejahatan siber keuangan kepada orang lain agar mereka tidak menjadi korban serangan kejahatan siber keuangan. 4. Saya termotivasi mengajak orang lain untuk menggunakan *software* perlindungan (antivirus) pada perangkat elektronnik untuk menghindari serangan kejahatan siber keuangan.	(Liang & Xue, 2009b), dengan modifikasi

3.4.9 Perilaku Penghindaran Kejahatan Siber Keuangan

Perilaku didefinisikan sebagai perbuatan atau tindakan seseorang untuk merespon suatu hal dan menjadikan tindakan tersebut sebagai kebiasaan karena terdapat nilai yang diyakini (Triwibowo, 2015). Perilaku penghindaran merupakan respon universal terhadap situasi bermuatan emosional yang paling sering dikaitkan

dengan kecemasan atau ketakutan. Perilaku penghindaran berupa tindakan apa pun untuk menghindari atau melarikan diri dari pikiran atau perasaan tertentu (Baker et al., 2016). Perilaku penghindaran juga dapat didefinisikan sebagai perilaku apapun yang dilakukan dengan tujuan mengalihkan diri dari situasi yang tidak diinginkan (Sheynin et al., 2014). Berdasarkan makna-makna tersebut, perilaku penghindaran dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menghindari suatu hal. Dari definisi yang telah disebutkan, maka perilaku penghindaran kejahatan siber keuangan dapat diartikan sebagai tindakan yang biasa dilakukan oleh seseorang untuk menjaga dirinya agar tidak menjadi korban kejahatan siber keuangan.

Berdasarkan pembahasan di atas, maka diajukan 6 pertanyaan untuk mengukur konstruk perilaku penghindaran kejahatan siber keuangan yang dikembangkan oleh (Liang & Xue, 2009a) dan (Verkijika, 2019). Adapun item pertanyaan yang dimaksud terdapat pada Tabel 3.9.

Tabel 3.9 Indikator Perilaku Penghindaran Kejahatan Siber Keuangan

Variabel	Item Pertanyaan	Referensi
Perilaku Penghindaran Kejahatan Siber Keuangan (Y)	1. Saya selalu memverifikasi seluruh email berasal dari sumber terpercaya sebelum membuka lampiran atau tautan apapun di perangkat elektronik saya. 2. Saya selalu memverifikasi keaslian pesan sebelum membuka tautan dari SMS atau *messaging platform* pada perangkat elektronik saya. (Misal: WhatsApp, Line, Facebook Messenger). 3. Saya hanya mengizinkan notifikasi (pemeberitahuan dari situs atau *software* terpercaya pada perangkat elektronik saya. 4. Seluruh *software* yang terpasang pada perangkat elektronik saya selalu berasal dari sumber terpercaya.	(Liang & Xue, 2009a) dan (Verkijika, 2019), dengan modifikasi

Variabel	Item Pertanyaan	Referensi
	5. Saya selalu memperbarui system operasi & seluruh *software* yang terpasang dalam perangkat elektronik secara berkala segera setelah pembaharuan tersedia. 6. Saya menjalankan *software* perlindungan perangkat elektronik (antivirus) secara teratur untuk menghindari serangan kejahatan siber keuangan di perangkat elektronik saya.	

3.5 Metode Analisis

Dalam penelitian ini, penulis menggunakan metode SEM-PLS dengan software SmartPLS untuk menganalisis data. *Partial Least Square* atau PLS merupakan model persamaan *Structure Equation Modelling* (SEM) dengan pendekatan yang didasari oleh varian atau *component-based structural equation modelling.* PLS digunakan untuk menejelaskan ada atau tidak adanya hubungan antar variabel laten (Hair et al., 2019). PLS juga merupakan metode analisis yang tidak mengasumsikan data arus dengan pengukuran skala tertentu dan dapat digunakan untuk menganalisis data dengan sampel yang kecil. Analisis data dalam penelitian ini menggunakan *software* SmartPLS karena penelitian ini memiliki model yang kompleks. Analisis dengan *software* SmartPLS menggunakan metode *bootstrapping* atau penggandaan secara acak sehingga asumsi normalitas tidak akan menjadi masalah. Analisis SEM-PLS terdiri dari dua sub model yaitu model pengukuran atau *outer model* dan model structural atau *inner model.* Model pengukuran menunjukan bagaimana variabel manifest atau *observed variable* merepresentasi variabel laten untuk diukur. Sedangkan model struktural menunjukan kekuatan estimasi antar variabel laten dan konstruk (Hair et al., 2019).

3.5.1 Uji Model Pengukuran

Uji model pengukuran dalam penelitian ini meliputi uji validitas dan reliabilitas. Tujuan pengujian ini adalah untuk mengukur sejauh mana tingkat validitas dan reliabilitas suatu model pengukuran penelitian.

3.5.1.1 Uji Validitas

Uji validitas digunakan untuk mengukur sah atau valid tidaknya suatu kuesioner. Suatu kuesioner dikatakan valid jika pertanyaan pada kuesioner mampu untuk mengungkapkan sesuatu yang akan diukur oleh kuesioner tersebut. Pengukuran validitas instrumen penelitian dilakukan dengan menguji *convergent validity* dan *discriminant validity*. Uji *convergent validity* dilakukan dengan menggunakan faktor analisis dan uji *discriminant validity* dilakukan dengan menggunakan *heterotrait-monotrait ratio* (HTMT).

Dengan *convergent validity,* model pengukuran dengan indicator refleksif dapat dilihat dari korelasi antar item indicator dengan skor konstruknya. Ukuran reflektif individual dikatakan tinggi jika berkorelasi lebih dari 0,70 dengan konstruk yang diukur. Namun demikian pada riset tahap pengembangan skala, apabila *loading cross* bernilai 0,50 sampai 0,60 masih dapat diterima (Hair et al., 2019).

Pada pengujian *discriminant validity,* rasio HTMT dipilih karena HTMT dianggap sebagai pengukuran yang lebih unggul daripada kriteria Fornell-Larcker yang umum digunakan (Henseler et al., 2015). HTMT merupakan rasio korelasi antar-sifat dengan korelasi dalam sifat. HTMT adalah *mean* dari semua korelasi indikator di seluruh konstruksi yang mengukur konstruksi yang berbeda (yaitu, korelasi heterotrait-heterometode) relatif terhadap *mean* (geometris) dari korelasi

rata-rata indikator yang mengukur konstruksi yang sama. Secara teknis, pendekatan HTMT adalah perkiraan tentang korelasi sebenarnya antara dua konstruk, jika keduanya diukur dengan sempurna (yaitu, jika keduanya dapat diandalkan secara sempurna). *Discriminant validity* dikonfirmasi mengikuti kriteria konservatif ketika nilai HTMT berada di bawah 0,90 (Henseler et al., 2015).

3.5.1.2 Uji Reliabilitas

Uji reliabilitas digunakan untuk menilai apakah data hasil angket atau kuesioner dapat dipercaya/reliabel atau tidak. Indikator untuk uji reliabilitas adalah *Cronbach Alpha*. Apabila nilai *Cronbach Alpha* $\alpha > 0,70$ maka berarti bahwa instrumen yang digunakan reliabel. Semakin dekat nilai Alpha kepada nilai 1 berarti pernyataan semakin reliabel. Uji reliabilitas dikatakan reliabel apabila semua variabel memiliki nilai Cronbach Alpha $\alpha > 0,70$ (Hair et al., 2019)

3.5.2 Uji Struktural

Uji struktural digunakan untuk menguji hubungan atau kekuatan estimasi antar variabel laten atau konstruk berdasarkan pada teori substantif. Model struktural menunjukan kekuatan estimasi antar variabel laten atau konstruk (Ghozali & Latan, 2015).

3.5.2.1 *R-Square*

Dalam menilai model struktural dengan PLS, dimulai dengan melihat nilai R-Squares untuk setiap variabel laten endogen sebagai kekuatan prediksi dari model struktural. Perubahan nilai R-Squares dapat digunakan untuk menjelaskan pengaruh variabel laten eksogen tertentu terhadap variabel laten endogen apakah mempunyai pengaruh yang substantive. Semakin tinggi nilai R-Square maka

semakin tinggi varibel eksogen dapat menjelaskan variasi variabel (Hair et al., 2019).

3.5.2.2 *Goodness of Fit*

Uji *Goodness of Fit* pada prinsipnya dilakukan untuk mengetahui apakah sebuah distribusi data dari sampel mengikuti sebuah distribusi teoritis tertentu atau tidak. Nilai GoF berada diantara 0 sampai dengan 1, dengan rekomendasi nilai communality 0,50 dan nilai *adjusted* R^2 dengan nilai interpretasi nilai GoF 0,10 (GoF *small*), nilai GoF 0,25 (GoF *medium*), nilai GoF 0,36 (GoF *large*) (Hair *et al.*, 2019).

3.5.2.3 *Estimate Path for Coefficients*

Uji selanjutnya adalah melihat signifikansi pengaruh antar variabel dengan melihat nilai koefisien parameter dan nilai signifikansi T statistik yaitu melalui metode *bootstrapping.* Prosedur *bootstrap* menggunakan seluruh sampel asli untuk melakukan resampling kembali. *Number of bootstrap samples* sebesar 200-1000 sudah cukup untuk mengoreksi standar *error estimate* PLS. Dalam metode resampling bootstrap, nilai signifikansi yang digunakan (two-tailed) t-value 1,65 (*significance level* = 10%), 1,96 (*significance level* = 5%) dan 2,58 (*significance level* = 1%) (Hair *et al.*, 2019).

BAB 4

HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian mengenai faktor-faktor yang mempengaruhi perilaku penghindaran kejahatan siber keuangan akan dianalisis dan dibahas pada bab ini. Informasi dari hasil pengolahan data akan digunakan untuk mengetahui hipotesis dapat diterima atau tidak.

4.1 Hasil Pengumpulan Data Penelitian

Hasil pengumpulan data pada penelitian ini menggunakan kuesioner secara *online (google form)* dan *offline (paper-based).* Pengambilan sampel dalam penelitian ini menggunakan metode *convenience sampling* dimana teknik tersebut dipilih karena peneliti tidak memiliki data terkait populasi dalam bentuk *sampling frame* dan peneliti kemudian memilih sampel berdasarkan prinsip kemudahan dalam mengambil atau memilih sampel. Sampel pada penelitian ini adalah pekerja industri sektor keuangan di Indonesia yang bekerja menggunakan perangkat elektronik. Kuesioner penelitian ini mulai dikumpulkan sejak tanggal 18 Maret 2023 hingga 10 Mei 2023.

Tabel 4.1 Hasil Pengumpulan Data

Keterangan	Jumlah		Presentase
Kuesioner *Offline*			
Kuesioner yang Disebar	45		100%
Kuesioner yang Tidak Kembali	6		13%
Kuesioner yang Tidak Memenuhi Syarat	2		4%
Kuesioner yang Kembali & Memenuhi Syarat		**37**	**82%**
Kuesioner *Online*			
Kuesioner yang Disebar	143		100%
Kuesioner yang Tidak Kembali	0		0%
Kuesioner yang Tidak Memenuhi Syarat	0		0%
Kuesioner yang Kembali & Memenuhi Syarat	**143**		**100%**

Keterangan	Jumlah	Presentase
Total Kuesioner yang Dapat Dianalisis	**180**	**96%**

Sumber: Data Diolah, 2023

Dari Tabel 4.1 dapat diketahui bahwa penelitian ini dilakukan dengan menyebarkan kuesioner *offline* sebanyak 45 buah (100%), dengan 6 buah (13%) kuesioner tidak kembali, dan 2 buah (4%) kuesioner tidak memenuhi syarat. Dari hasil pengumpulan data secara *offline* diperoleh 37 buah (82%) kuesioner yang dikembalikan oleh responden dan telah memenuhi syarat sehingga dapat dioleh dan dianalisis lebih lanjut. Sedangkan pengumpulan data secara *online* memperoleh respon sebanyak 143 buah (100%) kuesioner yang terisi dengan memenuhi syarat yang telah ditentukan. Hal tersebut berarti bahwa seluruh data yang diperoleh melalui kuesioner *online* dapat diolah dan dianalisis lebih lanjut.

4.2 Demografi Responden Penelitian

Pada bagian ini tersaji beberapa informasi demografi responden yang terkait dengan beberapa informasi umum seperti jenis kelamin, usia, kategori industri sektor keuangan tempat bekerja, wilayah tempat bekerja, lama bekerja, bidang profesi, dan pengalaman responden terkait serangan kejahatan siber keuangan.

4.2.1 Responden Berdasarkan Jenis Kelamin

Responden berdasarkan jenis kelamin dalam penelitian ini dapat dilihat pada Tabel 4.2

Tabel 4.2 Responden Berdasarkan Jenis Kelamin

	Jumlah	Persentase
Laki-laki	94	52%
Perempuan	86	48%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

4.2.2 Responden Berdasarkan Kelompok Usia

Responden berdasarkan kelompok usia dalam penelitian ini dapat dilihat pada Tabel 4.3

Tabel 4.3 Responden Berdasarkan Kelompok Usia

Rentang Usia	Jumlah	Persentase
< 20 tahun	0	0%
20-29 tahun	87	48%
30-39 tahun	52	29%
40-49 tahun	27	15%
50-59 tahun	14	8%
> 59 tahun	0	0%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Hasil pengumpulan data responden berdasarkan kelompok usia seperti pada tabel di atas dapat diketahui bahwa responden yang termasuk kelompok usia dari 20 tahun tidak ada atau sejumlah 0 orang (0%), responden yang termasuk kelompok usia 20-29 tahun sebanyak 87 orang (48%), responden yang termasuk kelompok usia 30-39 tahun sebanyak 52 orang (29%), responden yang termasuk kelompok usia 40-49 tahun sebanyak 27 orang (15%), responden yang termasuk kelompok uasia 50-59 tahun terdapat 14 orang (8%), dan tidak terdapat responden yang termasuk ke dalam kelompok usia > 59 tahun.

4.2.3 Responden Berdasarkan Sektor Industri

Responden berdasarkan sektor industri pekerjaan dalam penelitian ini dapat dilihat pada Tabel 4.4

Tabel 4.4 Responden Berdasarkan Sektor Industri Pekerjaan

Bekerja di Industri Sektor Keuangan		
	Jumlah	**Persentase**
Ya	180	100%

Bekerja di Industri Sektor Keuangan		
	Jumlah	**Persentase**
Tidak	0	0%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Dari Tabel 4.4 dapat dilihat bahwa seluruh responden sejumlah 180 orang (100%) bekerja pada perusahaan yang bergerak di sektor keuangan. Hal tersebut berarti bahwa seluruh responden telah memenuhi syarat sebagai sampel penelitian.

4.2.4 Responden Berdasarkan Kategori Sektor Industri Keuangan

Responden berdasarkan kategori sektor industri pekerjaan dalam penelitian ini dapat dilihat pada Tabel 4.5

Tabel 4.5 Kategori Sektor Industri Keuangan

Kategori Sektor Industri	Jumlah	Persentase
Perbankan	87	48%
Asuransi	25	14%
Perusahaan Sekuritas	14	8%
Lembaga Pembiayaan (Leasing, Anjak Piutang, dsb.)	22	12%
Koperasi Simpan Pinjam	3	2%
Pegadaian	2	1%
Lainnya	27	15%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Tabel 4.5 menunjukkan bahwa mayoritas responden bekerja pada industri perbankan yaitu sebanyak 87 responden atau 48% dari total keseluruhan responden. Responden yang berasal dari industri asuransi sebanyak 25 orang (14%), responden yang berasal dari perusahaan sekuritas sebanyak 14 orang (8%), dan responden yang berasal dari lembaga pembiayaan sebanyak 22 orang (12). Selain itu, sebanyak 3 responden (2%) berasal dari koperasi simpan pinjam, 2 orang responden (1%) berasal dari pegadaian, dan terdapat 27 orang (15%) yang berasal dari kategori sektor industri keuangan lainnya.

4.2.5 Responden Berdasarkan Wilayah Tempat Bekerja

Responden berdasarkan kategori sektor industri pekerjaan dalam penelitian ini dapat dilihat pada Tabel 4.6.

Tabel 4.6 Wilayah Tempat Bekerja

Provinsi	Jumlah	Persentase
DKI Jakarta	76	42%
Daerah Istimewa Yogyakarta	56	31%
Jawa Tengah	15	8%
Jawa Barat	13	7%
Jawa Timur	9	5%
Banten	3	2%
Sumatera Selatan	2	1%
Lampung	2	1%
Bali	1	1%
Gorontalo	1	1%
Kepulauan Riau	1	1%
Kalimantan Timur	1	1%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Tabel di atas menunjukkan hasil pengumpulan data yang diperoleh bahwa responden yang berasal dari DKI Jakarta berjumlah 76 orang atau 42%; Daerah Istimewa Yogyakarta sejumlah 56 orang atau 31%; Jawa Tengah sebanyak 15 orang atau 8%; Jawa Barat sejumlah 13 orang atau 7%; Jawa Timur sejumlah 9 orang atau 5%; Banten sebanyak 3 orang atau 2%; Sumatera Selatan & Lampung masing-masing sejumlah 2 orang atau 1%; serta Bali, Gorontalo, Kepulauan Riau, dan Kalimantan Timur dengan masing-masing sejumlah 1 orang atau 1%.

4.2.6 Responden Berdasarkan Lama Bekerja

Responden berdasarkan kategori sektor industri pekerjaan dalam penelitian ini dapat dilihat pada Tabel 4.7.

Tabel 4.7 Lama Bekerja

Rentang Tahun	Jumlah	Persentase
1-3 tahun	51	28%
4-7 tahun	44	24%
7-10 tahun	24	13%
>10 tahun	61	34%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Tabel 4.7 menunjukkan bahwa responden dalam penelitian ini terdiri dari 51 orang (28%) yang telah bekerja selama 1-3 tahun, 44 orang (24%) yang telah bekerja selama 4-7 tahun, 24 orang (13%) yang telah bekerja selama 7-10 tahun, dan 61 orang (34%) yang telah bekerja selama lebih dari 10 tahun.

4.2.7 Responden Berdasarkan Bidang Profesi

Responden berdasarkan bidang profesi dalam penelitian ini dapat dilihat pada Tabel 4.7 yang tersaji berikut ini.

Tabel 4.7 Bidang Profesi Responden

Bidang profesi	Jumlah	Persentase
Akuntansi & Keuangan	63	35%
Administrasi	16	9%
General Affair	2	1%
HRD	11	6%
Pemasaran & Penjualan	18	10%
Teknologi Informasi	10	6%
Lainnya	60	33%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Dari tabel di atas dapat dilihat bahwa 63 responden atau 35% responden berprofesi di bidang akuntansi & keuangan, 16 responden atau 9% responden berprofesi di bidang administrasi, 2 orang atau 1% responden berprofesi di bidang *general affair*, 11 orang atau 6% responden berprofesi sebagai HRD, 18 orang atau 10% responden berprofesi di bidang pemasaran & penjualan, 10 orang atau 6%

responden berprofesi di bidang teknologi informasi, dan 60 orang atau 33% responden berprofesi di bidang lainnya.

4.2.8 Responden Berdasarkan Penggunaan Perangkat Elektronik Dalam Bekerja

Responden berdasarkan penggunaan perangkat elektronik dalam bekerja pada penelitian ini dapat dilihat pada Tabel 4.8.

Tabel 4.8 Penggunaan Perangkat Elektronik Dalam Bekerja

	Jumlah	Persentase
Ya	180	100%
Tidak	0	0%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Tabel 4.8 menunjukkan bahwa seluruh responden dalam penelitian ini menggunakan perangkat elektronik dalam bekerja. Oleh karena itu, seluruh kuesioner dalam penelitian ini telah memenuhi syarat untuk dilakukan analisis lebih lanjut.

4.2.9 Responden Berdasarkan Pengalaman Terkait Serangan Kejahatan Siber Keuangan

Responden berdasarkan pengalaman menjadi korban kejahatan siber keuangan pada penelitian ini dapat dilihat pada Tabel 4.9.

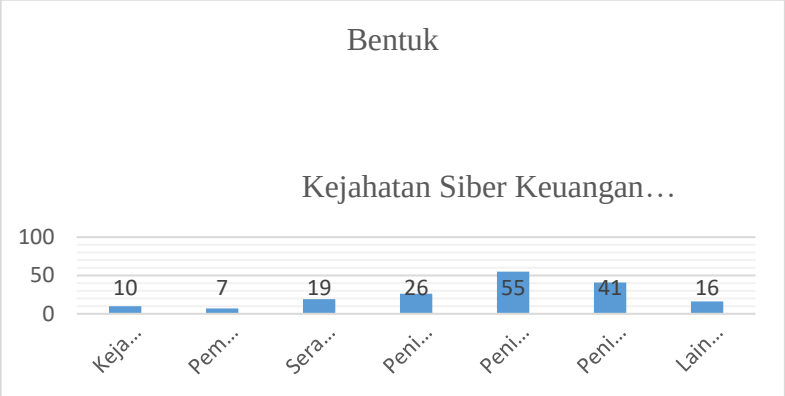
Tabel 4.9 Pengalaman Menjadi Korban Kejahatan Siber Keuangan

	Jumlah	Persentase
Pernah	68	38%
Tidak Pernah	112	62%
Total	**180**	**100%**

Sumber: Data Diolah, 2023

Tabel di atas menunjukkan bahwa 68 orang atau 38% responden pernah menjadi korban kejahatan siber keuangan dan 112 orang atau 62% responden tidak

pernah menjadi korban kejahatan siber keuangan. Adapun bentuk serangan kejahatan siber keuangan yang pernah dialami oleh responden tersaji dalam grafik berikut ini.



Grafik 4.1 Bentuk Kejahatan Siber Keuangan yang Pernah Dialami oleh Responden

4.3 Uji Instrumen Penelitian

Uji instrumen yang dilakukan pada penelitian meliputi uji validitas dan reliabilitas, yang bertujuan untuk mengukur sejauh mana tingkat validitas dan reliabilitas pada masing-masing instrumen penelitian.

4.3.1 Uji Validitas

4.3.1.1 Uji Validitas Konvergen (*Convergent Validity*)

Uji Validitas Konvergen pada penlitian ini dilakukan dengan menggunakan software SmartPLS 4. Uji ini merupakan sebuah indikator dari konstruk yang harus konvergen (akurat) atau memiliki proporsi varians yang tinggi pada suatu variabel (Hair *et al*., 2019). Uji validitas konvergen ini dapat dilihat melalui nilai loading dari masing-masing instrumen dengan *average variance extracted* (AVE). Untuk memenuhi uji tersebut, maka nilai *outer loadings factor* harus lebih besar dari 0,6. Nilai AVE harus lebih besar dari 0,5. Hal itu

menunjukkan bahwa dalam rata-ratanya konstruk telah mampu menjelaskan setengah dari varians indikatornya (Hair *et al*., 2017). Hasil uji validitas konvergen disajikan dalam Tabel 4.10.

Tabel 4.10 Uji Validitas Konvergen Awal

Variabel	Kode	Loading	AVE	Keterangan
Persepsi Kerentanan	PKR1	0.872	0.760	Valid
	PKR2	0.894		
	PKR3	0.849		
Persepsi Keparahan	PKP1	0.889	0.713	Valid
	PKP2	0.897		
	PKP3	0.737		
Persepsi Ancaman	PA1	0.877	0.654	Valid
	PA2	0.899		
	PA3	0.772		
	PA4	0.664		
Efikasi Diri	ED1	0.817	0.775	Valid
	ED2	0.916		
	ED3	0.909		
	ED4	0.875		
Efektivitas Perlindungan	ED1	0.912	0.858	Valid
	ED2	0.957		
	ED3	0.910		
Safeguard Cost	SC1	0.764	**0.312**	**Tidak Valid**
	SC2	0.788		
	SC3	**0.087**		
	SC4	**-0.195**		
Antisipasi Penyesalan	AP1	0.816	0.685	Valid
	AP2	0.798		
	AP3	0.868		
Motivasi Penghindaran Kejahatan Siber Keuangan	MP1	0.773	0.655	Valid
	MP2	0.862		
	MP3	0.760		
	MP4	0.837		
Perilaku Penghindaran Kejahatan Siber Keuangan	PP1	0.837	0.618	Valid
	PP2	0.859		
	PP3	0.772		
	PP4	0.760		
	PP5	0.789		
	PP6	0.685		

Tabel 4.10 di atas menunjukkan bahwa seluruh item kuesioner untuk masing-masing variabel ada yang memiliki nilai *loading* > 0.5 namun ada juga yang memiliki nilai *loading* < 0.5. Item kuesioner yang memiliki nilai *loading* < 0,5 yaitu item kuesioner SC3 yang memiliki nilai 0.087 dan item kuesioner SC4 yang memiliki nilai -0.915. Berdasarkan hal tersebut, item SC3 dan SC4 pada variabel *Safeguard Cost* harus dihapus karena memiliki nilai *loading* < 0.5. Pengujian ulang dilakukan dengan mengeluarkan item yang memiliki nilai *loading* < 0.5 agar nilai AVE menjadi minimal sama dengan 0.5. Hasil pengujian ulang dapat dilihat pada Tabel 4.11 di bawah ini.

Tabel 4.11 Uji Validitas Konvergen Akhir

Variabel	Kode	Loading	AVE	Keterangan
Persepsi Kerentanan	PKR1	0.872	0.760	Valid
	PKR2	0.894		
	PKR3	0.849		
Persepsi Keparahan	PKP1	0.889	0.713	Valid
	PKP2	0.897		
	PKP3	0.737		
Persepsi Ancaman	PA1	0.877	0.654	Valid
	PA2	0.899		
	PA3	0.772		
	PA4	0.664		
Efikasi Diri	ED1	0.817	0.775	Valid
	ED2	0.916		
	ED3	0.909		
	ED4	0.875		
Efektivitas Perlindungan	ED1	0.912	0.858	Valid
	ED2	0.957		
	ED3	0.910		
Safeguard Cost	SC1	0.906	0.879	Valid
	SC2	0.968		
Antisipasi Penyesalan	AP1	0.816	0.685	Valid
	AP2	0.798		
	AP3	0.868		
Motivasi Penghindaran	MP1	0.775	0.655	Valid
	MP2	0.863		

Variabel	Kode	Loading	AVE	Keterangan
Kejahatan Siber Keuangan	MP3	0.759		
	MP4	0.853		
Perilaku Penghindaran Kejahatan Siber Keuangan	PP1	0.837	0.618	Valid
	PP2	0.859		
	PP3	0.772		
	PP4	0.760		
	PP5	0.790		
	PP6	0.685		

Data yang tersaji pada Tabel 4.11 menunjukkan bahwa setelah menghapus dua item indikator kuesioner pada variabel *Safeguard Cost*, seluruh indikator variabel memiliki nilai *outer loading* lebih besar dari 0,6 dan setiap variabel memiliki nilai AVE lebih dari 0,5. Dari data tersebut, dapat disimpulkan bahwa seluruh variabel telah memenuhi kriteria *loading factor* sehingga variabel dalam penelitian ini telah dikatakan valid. Dengan demikian, pada pengujian selanjutnya pengukuran variabel *safeguard cost* hanya menggunakan dua item indikator.

4.3.1.2 Uji Validitas Diskriminan

Uji validitas diskriminan dalam penelitian ini dilakukan dengan menggunakan metode Heterotrait Monotrait (HTMT). *Discriminant validity* dikonfirmasi mengikuti kriteria konservatif ketika nilai HTMT berada di bawah 0,90 (Henseler et al., 2015).

Tabel 4.12 Hasil Uji HTMT

	AR	SFE	SLE	AM	AB	PT	PSV	PSC	SC	PSC X PSV
AR										
SFE	0.395									
SLE	0.093	0.285								
AM	0.707	0.381	0.162							
AB	0.418	0.460	0.390	0.621						
PT	0.506	0.309	0.060	0.528	0.480					
PSV	0.540	0.352	0.067	0.506	0.397	0.862				
PSC	0.430	0.166	0.125	0.362	0.189	0.708	0.864			
SC	0.123	0.121	0.069	0.135	0.177	0.331	0.252	0.303		
PSC X PSV	0.112	0.110	0.029	0.090	0.116	0.454	0.521	0.477	0.040	

Tabel 4.12 menyajikan hasil uji validitas diskriminan menggunakan metode HTMT dimana seluruh hasil memiliki nilai < 0,90. Nilai tertinggi yang terdapat pada tabel tersebut adalah 0.864. Oleh karena itu seluruh variabel dapat dikatakan valid.

4.3.2 Uji Reliabilitas

Uji reliabilitas dari konstruk-konstruk yang ada dapat dilihat dari nilai *cronbach's alpha* dan *composite reliability* dari masing-masing konstruk. Didalam software SmartPLS 4 terdapat dua cara yaitu *cronbach's alpha* dan *composite reliability* (Hair *et al*., 2019). Karena keterbatasan *cronbach's alpha*, secara teknis akan lebih tepat menggunakan *composite reliability* untuk menerapkan ukuran yang menghasilkan nilai reliabilitas yang cenderung melebih-lebihkan keandalan konsistensi internal (Hair *et al*., 2017).

Nilai *composite reliability* bervariasi antara 0 sampai dengan 1, semakin tinggi nilainya menunjukkan bahwa tingkat reliabilitasnya lebih tinggi. Suatu variabel dikatakan reliabel dapat dilihat dari nilai *composite reliability* dan nilai

cronbach's alpha. Nilai *composite reliability* yang baik memiliki nilai diatas 0,7 dan nilai *cronbach's alpha* yang direkomendasikan lebih tinggi dari 0,7. Berikut merupakan nilai *composite reliability* dan *cronbach's alpha* dari masing-masing konstruk yang disajikan pada Tabel 4.13

Tabel 4.13 Uji Reliabilitas

Variabel	*Composite Reliability*	*Cronbach's Alpha*	Keterangan
Persepsi Kerentanan (PKR)	0.905	0.842	Reliabel
Persepsi Keparahan (PKP)	0.881	0.794	Reliabel
Persepsi Ancaman (PA)	0.882	0.823	Reliabel
Efikasi Diri (ED)	0.932	0.902	Reliabel
Efektivitas Perlindungan (EP)	0.948	0.918	Reliabel
Safeguard Cost (SC)	0.936	0.871	Reliabel
Antisipasi Penyesalan (AP)	0.867	0.772	Reliabel
Motivasi Penghindaran Kejahatan Siber Keuangan (MP)	0.883	0.824	Reliabel
Perilaku Penghindaran Kejahatan Siber Keuangan (PP)	0.906	0.876	Reliabel

Berdasarkan tabel di atas, dapat dilihat bahwa nilai *composite reliability* keseluruhan variabel memiliki nilai lebih dari 0,7 dan nilai cronbach's alpha lebih dari 0,7. Sehingga dapat ditarik kesimpulan bahwa seluruh variabel sangat reliabel dan seluruh konstruk dalam penelitian ini dinyatakan dapat diandalkan.

4.4 Uji Model Struktur

Model struktur merupakan hubungan yang menggambarkan anatara variabel laten berdasarkan teori substantive atau variable yang telah dihipotesiskan sebelumnya. Penilaian model struktural dapat dilakukan dengan mengavaluasi signifikansi statistik dari *path loading* (nilai-t) dan *path coefficient* (β) antara setiap konstruk, serta jumlah varian yang dijelaskan atau *R-Squared* (R^2). Dalam

melakukan analisis menggunakan PLS sebagai alat analisis dengan menjalankan prosedur *bootstrapping*.

4.4.1 Uji *R-Square* (R^2)

Uji *R-Square* digunakan untuk mengukur besarnya kemampuan model dalam menjelaskan variabel dependen. Nilai *R-Square* berkisar antara 0 sampai 1, semakin tinggi hasil yang diperoleh menunjukkan tingkat akurasi prediksi semakin tinggi. Hasil nilai *R-Square* dapat dilihat pada Tabel 4.14.

Tabel 4.14 Nilai *R-Square*

Variabel	*R-Square*	*R-Square Adjusted*
Persepsi Ancaman	0.545	0.537
Motivasi Penghindaran Kejahatan Siber Keuangan	0.391	0.374
Perilaku Penghindaran Kejahatan Siber Keuangan	0.294	0.290

Tabel di atas menunjukkan bahwa variabel Persepsi Ancaman memiliki nilai *R-Square* sebesar 0,545 yang berarti bahwa konstruk Persepsi Kerentanan (PKR) dan Persepsi Keparahan (PKP) mempengaruhi konstruk Persepsi Ancaman (PA) sebesar 50,45%, sedangkan sisanya sebesar 49,65% dijelaskan oleh konstruk lainnya. Variabel Motivasi Penghindaran Kejahatan Siber Keuangan memiliki nilai *R-Square* sebesar 0,391 yang berarti bahwa konstruk Persepsi Ancaman (PA), Efikasi Diri (ED), Efektivitas Perlindungan (EP), *Safeguard Cost* (SC), dan Antisipasi Penyesalan (AP) mempengaruhi konstruk Motivasi Penghindaran Kejahatan Siber Keuangan (MP) sebesar 30,91% sedangkan sisanya sebesar 69,09% dijelaskan oleh konstruk lainnya. Variabel Perilaku Penghindaran Kejahatan Siber Keuangan memiliki nilai *R-Square* sebesar 0,294 yang berarti bahwa konstruk Motivasi Penghindaran Kejahatan Siber Keuangan mempengaruhi

konstruk Perilaku Penghindaran Kejahatan Siber Keuangan sebesar 20,94% sedangkan sisanya sebesar 70,06% dipengaruhi oleh konstruk lainnya.

4.4.2 Hasil Uji *Goodnes of Fit* (GoF)

Uji *Goodness of Fit* (GoF) dilakukan dengan cara mengakar kuadratkan hasil perkalian antara nilai rata-rata AVE dengan nilai rata-rata *R-Square*. Data VE dan *R-Square* disajikan pada Tabel 4.15.

Tabel 4.15 Nilai AVE dan *R-Squared*

Variabel	AVE	*R-Square*
Antisipasi Penyesalan	0,685	0,545
Motivasi Penghindaran Kejahatan Siber Keuangan	0,655	0,391
Perilaku Penghindaran Kejahatan Siber Keuangan	0,618	0,294

Sumber: Data Diolah, 2023

Dari total rata-rata yang diperoleh pada Tabel 4.14, jika GoF sebesar 0,1 maka dapat dikategorikan GoF kecil. Jika diperoleh GoF sebesar 0,25 maka dapat dikategorikan GoF sedang. Sementara jika diperoleh GoF sebesar 0,36 maka dapat dikategorikan GoF besar (Cohen, 1988). Untuk mengetahui seberapa besar nilai GoF yang diperoleh dengan cara perhitungan sebagai berikut:

$$\text{GoF} = \sqrt{\overline{AVE} \; x \; \overline{R^2}}$$

$$\text{GoF} = \sqrt{0{,}653 \; x \; 0{,}410}$$

$$\text{GoF} = 0{,}517$$

Berdasarkan perhitungan di atas, maka diperoleh nilai GoF sebesar 0,517. Nilai GoF sebesar 0,517 tergolong kategori GoF besar. Maka dari itu, dapat disimpulkan bahwa pada penelitian ini memiliki model penelitian yang kuat.

4.4.3 Hasil Uji *Path Coefficient* dan *Statistical Significance*

Setelah penilaian kekuatan penjelas dari model penelitian melalui jumlah varians yang dijelaskan oleh nilai R^2 dan kekuatan model telah dianalisis dengan metode GoF, maka selanjutnya dilakukan evaluasi hipotesis konstruk dalam penelitian ini. Analisis ini dilakukan dengan mengevaluasi nilai *path coefficient* dan signifikansi statistik dari nilai t (t-statistik). Tabel 4.16 menunjukkan hasil pengujian tersebut yang dilakukan dengan prosedur *bootstrapping*.

Tabel 4.16 Hasil Uji *Path Coefficient* dan *Statistical Significance*

	Coefficient Value (Beta)	***Standard Deviation (STDEV)***	***T Statistics***	***P Values***	**Hasil**
PKR → PA	0.192	0.093	2.079	0.038*	Didukung
PKP → PA	0.548	0.085	6.476	0.000*	Didukung
PKR x PKP → PA	-0.050	0.074	0.671	0.503	Tidak Didukung
PA → MP	0.224	0.077	2.930	0.003*	Didukung
ED → MP	0.092	0.063	1.461	0.144	Tidak Didukung
EP → MP	0.117	0.069	1.685	0.092***	Didukung
SC → MP	-0.008	0.070	0.115	0.908	Tidak Didukung
AP → MP	0.426	0.093	4.563	0.000*	Didukung
MP → PP	0.542	0.064	8.524	0.000*	Didukung

Nilai signifikansi: *p < 0.05; ** p < 0.01; ***p < 0.1
Sumber: Data Diolah, 2023

Pengaruh Persepsi Kerentanan Terhadap Persepsi Ancaman

Besarnya koefisien parameter untuk variabel Persepsi Kerentanan (PKR) terhadap Persepsi Ancaman (PA) adalah sebesar 0,192 yang berarti terdapat pengaruh positif PKR terhadap PA. Hal tersebut juga berarti bahwa semakin tinggi persepsi kerentanan yang diyakini oleh seseorang maka persepsi ancaman yang dirasakan juga semakin tinggi. Berdasarkan perhitungan menggunakan *bootstrap* atau *resampling*, dimana hasil uji koefisien estimasi PKR terhadap PA memiliki

hasil 0.192, dengan nilai t hitung sebesar 2.079 dan standar deviasi sebesar 0.093 maka nilai *p-value* adalah sebesar 0.038 < 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Persepsi Kerentanan memiliki pengaruh secara positif signifikan terhadap Persepsi Ancaman. Oleh karena itu, Hipotesis 1 (H1) dinyatakan diterima.

Pengaruh Persepsi Keparahan Terhadap Persepsi Ancaman

Besarnya koefisien parameter untuk variabel Persepsi Keparahan (PKP) terhadap Persepsi Ancaman (PA) adalah sebesar 0,548 yang berarti terdapat pengaruh positif PKP terhadap PA. Hal tersebut juga berarti bahwa semakin tinggi persepsi keparahan yang diyakini oleh seseorang maka semakin tinggi juga persepsi ancaman yang mereka yakini. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling*, dimana hasil uji koefisien estimasi PKP terhadap PA memiliki hasil sebesar 0,548, dengan nilai t hitung sebesar 6,476 dan standar deviasi sebesar 0,085 maka nilai *p-value* sebesar 0.000 < 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Persepsi Keparahan memiliki pengaruh secara positif signifikan terhadap Persepsi Ancaman. Oleh karena itu, hipotesis 2 (H2) dinyatakan diterima.

Pengaruh Interaksi Antara Persepsi Kerentanan dan Persepsi Keparahan Terhadap Persepsi Ancaman

Besarnya koefisien parameter untuk interaksi antara variabel Persepsi Kerentanan dan Persepsi Keparahan (PKR x PKP) terhadap Persepsi Ancaman (PA) adalah sebesar -0,050 yang berarti terdapat pengaruh negatif PKRxPKP

terhadap PA. Hal tersebut juga berarti bahwa semakin tinggi interaksi antara persepsi kerentanan dan persepsi keparahan yang diyakini oleh seseorang, maka persepsi ancaman yang diyakini akan semakin rendah. Berdasarkan perhitungan menggunakan metode *bootstrap* atau *resampling*, dimana jadil uji koefisien estimasi PKRxPKP terhadap PA memiliki hasil -0,050, dengan nilai t hitung sebesar 0.671 dan standar deviasi sebesar 0,074 maka nilai *p-value* sebesar 0,503 > 0,05. Dari hasil tersebut, dapat disimpulkan bahwa interaksi antara Persepsi Kerentanan dan Persepsi Keparahan memiliki pengaruh secara negatif tidak signifikan terhadap Persepsi Ancaman. Oleh karena itu, hipotesis 3 (H3) dinyatakan tidak diterima.

Pengaruh Persepsi Ancaman Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel Persepsi Ancaman (PA) terhadap Motivasi Penghindaran Kejahatan Siber Keuangan (MP) adalah sebesar 0,224 yang berarti terdapat pengaruh positif PA terhadap MP. Hal tersebut juga berarti bahwa semakin tinggi persepsi ancaman yang diyakini oleh seseorang maka semakin tinggi juga motivasi seseorang untuk menghindari kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling*, dimana hasil uji koefisien estimasi PA terhadap MP memiliki hasil sebesar 0,224, dengan nilai t hitung sebesar 2,930 dan standar deviasi sebesar 0,077 maka nilai *p-value* sebesar 0.003 < 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Persepsi Ancaman memiliki pengaruh secara positif signifikan terhadap Motivasi

Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 4 (H4) dinyatakan diterima.

Pengaruh Efikasi Diri Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel Efikasi Diri (ED) terhadap Motivasi Penghindaran Kejahatan Siber Keuangan (MP) adalah sebesar 0,092 yang berarti terdapat pengaruh positif ED terhadap MP. Hal tersebut juga berarti bahwa semakin tinggi efikasi diri seseorang maka semakin tinggi juga motivasi seseorang untuk menghindari kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling,* dimana hasil uji koefisien estimasi ED terhadap MP memiliki hasil sebesar 0,092, dengan nilai t hitung sebesar 1,461 dan standar deviasi sebesar 0,063 maka nilai *p-value* sebesar 0.144 > 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Efikasi Diri memiliki pengaruh secara positif tidak signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 5 (H5) dinyatakan tidak diterima.

Pengaruh Efektivitas Perlindungan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel Efektivitas Perlindungan (EP) terhadap Motivasi Penghindaran Kejahatan Siber Keuangan (MP) adalah sebesar 0,117 yang berarti terdapat pengaruh positif EP terhadap MP. Hal tersebut juga berarti bahwa semakin tinggi efektivitas perlidungan yang dirasakan oleh seseorang maka semakin tinggi juga motivasi seseorang untuk menghindari kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling,*

dimana hasil uji koefisien estimasi EP terhadap MP memiliki hasil sebesar 0,117 dengan nilai t hitung sebesar 1,685 dan standar deviasi sebesar 0,069 maka nilai *p-value* sebesar 0.092 < 0.10. Dari hasil tersebut, dapat disimpulkan bahwa Efektivitas Perlindungan memiliki pengaruh secara positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 6 (H6) dinyatakan diterima.

Pengaruh *Safeguard Cost* Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel *Safeguard Cost* (SC) terhadap Motivasi Penghindaran Kejahatan Siber Keuangan (MP) adalah sebesar -0,008 yang berarti terdapat pengaruh negatif SC terhadap MP. Hal tersebut juga berarti bahwa semakin tinggi *safeguard cost* yang harus dikeluarkan oleh seseorang maka semakin rendah motivasi seseorang untuk menghindari kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling*, dimana hasil uji koefisien estimasi SC terhadap MP memiliki hasil sebesar -0,008 dengan nilai t hitung sebesar 0,115 dan standar deviasi sebesar 0,070 maka nilai *p-value* sebesar 0.908 > 0.05. Dari hasil tersebut, dapat disimpulkan bahwa *Safeguard Cost* memiliki pengaruh secara negatif tidak signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 7 (H7) dinyatakan tidak diterima.

Pengaruh Antisipasi Penyesalan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel Antisipasi Penyesalan (AP) terhadap Motivasi Penghindaran Kejahatan Siber Keuangan (MP) adalah sebesar 0,426 yang berarti terdapat pengaruh positif AP terhadap MP. Hal tersebut juga berarti bahwa semakin tinggi antisipasi penyesalan oleh seseorang maka semakin tinggi juga motivasi seseorang untuk menghindari kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling*, dimana hasil uji koefisien estimasi PA terhadap MP memiliki hasil sebesar 0,426 dengan nilai t hitung sebesar 4,563 dan standar deviasi sebesar 0,093 maka nilai *p-value* sebesar 0.000 < 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Antisipasi Penyesalan memiliki pengaruh secara positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 8 (H8) dinyatakan diterima.

Pengaruh Motivasi Penghindaran Kejahatan Siber Keuangan Terhadap Perilaku Penghindaran Kejahatan Siber Keuangan

Besarnya koefisien parameter untuk variabel Motivasi Penghindaran Kejahatan Siber Keuangan (MP) terhadap Perilaku Penghindaran Kejahatan Siber Keuangan (PP) adalah sebesar 0,542 yang berarti terdapat pengaruh positif MP terhadap PP. Hal tersebut juga berarti bahwa semakin tinggi motivasi penghindaran kejahatan siber keuangan oleh seseorang maka semakin tinggi juga perilaku penghindaran kejahatan siber keuangan. Berdasarkan perhitungan menggunakan *bootstrap* dan *resampling*, dimana hasil uji koefisien estimasi MP terhadap PP memiliki hasil sebesar 0,542 dengan nilai t hitung sebesar 8,524 dan standar deviasi

sebesar 0,064 maka nilai *p-value* sebesar 0.000 < 0.05. Dari hasil tersebut, dapat disimpulkan bahwa Motivasi Penghindaran Kejahatan Siber Keuangan memiliki pengaruh secara positif signifikan terhadap Perilaku Penghindaran Kejahatan Siber Keuangan. Oleh karena itu, hipotesis 9 (H9) dinyatakan diterima.

4.5 Pembahasan

4.5.1 Pengaruh Persepsi Kerentanan Terhadap Persepsi Ancaman

Hipotesis pertama (H1) menguji hubungan antara persepsi kerentanan terhadap persepsi ancaman. Hipotesis 1 menyatakan bahwa persepsi kerentanan berpengaruh positif terhadap persepsi ancaman. Hasil analisis koefisien jalur dan *statistical significance* menunjukkan bahwa persepsi kerentanan memiliki pengaruh secara positif dan signifikan terhadap persepsi ancaman. Oleh karena itu, hipotesis pertama dalam penelitian ini **diterima.**

Hipotesis pertama diterima karena apabila seseorang merasa rentan terhadap serangan kejahatan siber keuangan, mereka cenderung akan lebih peka dengan risiko atau bahaya yang mungkin akan terjadi. Ketika seseorang meyakini bahwa banyak risiko yang dapat terjadi di masa depan, untuk menghindarinya mereka akan meningkatkan persepsi ancaman yang mereka yakini. Hasil penelitian ini sejalan dengan penelitian yang dilakukan oleh (Sylvester, 2022) yang menunjukkan bahwa persepsi kerentanan berpengaruh terhadap persepsi ancaman atas serangan *phishing.* Selain itu, penelitian yang dilakukan oleh (Mark et al., 2021) terhadap 170 warga AS yang merupakan pengguna computer juga menunjukkan bahwa persepsi kerentanan berpengaruh positif signifikan terhadap persepsi ancaman serangan *phishing*.

Implikasi dari hasil penelitian ini adalah apabila seseorang merasa rentan terhadap serangan atau kejahatan siber keuangan, mereka cenderung akan mengambil langkah-langkah perlindungan tambahan atau bahkan menghindari penggunaan teknologi tersebut. Hal tersebut dikarenakan mereka cenderung lebih memperhatikan dan memperhitungkan konsekuensi negatif yang dapat timbul akibat serangan atau kejahatan siber keuangan. Ketika persepsi kerentanan terkait kejahatan siber keuangan cukup tinggi, maka pemerintah harus memperhatikan dan mempertimbangkan faktor-faktor yang mempengaruhi persepsi kerentanan dalam merumuskan kebijakan dan tindakan yang berkaitan dengan kemanan siber. Apabila seseorang merasa rentan terhadap ancaman kejahatan siber, mereka akan lebih memperhatikan dan mengikuti tindakan keamanan yang direkomendasikan oleh pemerintah atau organisasi terkait.

4.5.2 Pengaruh Persepsi Keparahan Terhadap Persepsi Ancaman

Hipotesis kedua (H2) menguji hubungan antara persepsi keparahan dengan persepsi ancaman. Hipotesis 2 menyatakan bahwa persepsi keparahan berpengaruh positif terhadap persepsi ancaman. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa persepsi keparahan memiliki pengaruh secara positif dan signifikan terhadap persepsi ancaman. Oleh karena itu, hipotesis kedua dalam penelitian ini **diterima.**

Ketika seseorang menganggap bahwa kejahatan siber keuangan akan mengakibatkan ancaman kejahatan siber keuangan merupakan salah satu hal yang serius, maka ia akan merasa terancam. Hasil penelitian ini sejalan dengan penelitian yang dilakukan oleh (Carpenter *et al.*, 2019) yang membuktikan bahwa persepsi

keparahan berpengaruh positif terhadap persepsi ancaman mereka atas serangan *phishing.* Selain itu, juga terdapat penelitian oleh (Sylvester, 2022) yang menunjukkan bahwa persepsi keparahan memiliki pengaruh positif signifikan terhadap persepsi ancaman.

Implikasi dari hasil penelitian ini adalah apabila persepsi keparahan tinggi, maka pemerintah harus merumuskan kebijakan dan tindakan penanggulangan yang lebih serius dan komprehensif yang dapat diimplementasikan untuk mengatasi kejahatan siber keuangan.

4.5.3 Pengaruh Interaksi Antara Persepsi Kerentanan dan Persepsi Keparahan Terhadap Persepsi Ancaman

Hipotesis ketiga (H3) menguji hubungan antara interaksi persepsi kerentanan dan persepsi keparahan dengan persepsi ancaman. Hipotesis 3 menyatakan bahwa interaksi antara persepsi kerentanan dan persepsi keparahan berpengaruh positif terhadap persepsi ancaman. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa interaksi antara persepsi kerentanan dan persepsi keparahan memiliki pengaruh secara negatif namun tidak signifikan terhadap persepsi ancaman. Hal tersebut juga dapat diartikan bahwa tidak terdapat interaksi antara persepsi kerentanan dan persepsi keparahan dalam mempengaruhi persepsi ancaman. Oleh karena itu, hipotesis ketiga dalam penelitian ini **tidak diterima.**

Tidak adanya interaksi antara persepsi kerentanan dan persepsi keparahan dalam mempengaruhi persepsi ancaman ini dikarenakan ketika seseorang berpikir

bahwa mereka rentan terhadap serangan kejahatan siber keuangan, disaat yang sama mereka percaya bahwa kerentanan tersebut tidak akan mengakibatkan suatu hal yang parah. Selain itu, persepsi ancaman adalah suatu hal yang sangat subjektif, artinya persepsi ancaman dipengaruhi oleh interpretasi dan penilaian individu terhadap situasi atau ancaman tertentu. Seseorang dapat menganggap dirinya rentan terhadap kejahatan siber keuangan, tetapi pada saat yang sama merasa dirinya dapat mengendalikan responnya agar tidak menyebabkan suatu hal yang parah.

Hasil ini berbeda dengan penelitian (Sylvester, 2022) yang menunjukkan bahwa interaksi antara persepsi kerentanan dan persepsi keparahan berpengaruh positif terhadap persepsi ancaman. Meskipun persepsi kerentanan dan persepsi keparahan merupakan faktor utama dalam membentuk persepsi ancaman, dalam penelitian ini menunjukkan bahwa tidak ada interaksi langsung antara keduanya. Hal tersebut berarti bahwa persepsi kerentanan dan persepsi keparahan berpengaruh terhadap persepsi ancaman secara independen. Implikasi dari hasil penelitian ini adalah dalam situasi di mana persepsi keparahan tidak memperkuat persepsi kerentanan, perusahaan sektor keuangan atau lembaga terkait perlu untuk menambah frekuensi edukasi terhadap pentingnya keamanan siber, meningkatkan kesadaran para karyawan perusahaan sektor keuangan akan bahaya ancaman kejahatan siber keuangan, dan meningkatkan pemahaman karyawan perusahaan sektor keuangan untuk merespon ancaman dengan efektif.

4.5.4 Pengaruh Persepsi Ancaman Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Hipotesis keempat (H4) menguji hubungan antara persepsi ancaman dengan motivasi penghindaran kejahatan siber keuangan. Hipotesis 4 menyatakan bahwa persepsi ancaman berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa persepsi ancaman memiliki pengaruh secara positif dan signifikan terhadap motivasi penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis keempat dalam penelitian ini **diterima.**

Persepsi ancaman yang tinggi dapat meningkatkan tingkat kewaspadaan pekerja sektor keuangan terhadap potensi kejahatan siber keuangan. Para pekerja sektor keuangan akan lebih waspada sehingga mereka akan termotivasi untuk melakukan tindakan penghindaran kejahatan siber keuangan. Hal tersebut sejalan dengan penelitian yang dilakukan oleh (Carpenter *et al.*, 2019) yang membuktikan bahwa persepsi ancaman berpengaruh positif terhadap motivasi penghindaran ancaman teknologi.

Situasi dimana tingkat persepsi ancaman tinggi, seseorang cenderung lebih termotivasi untuk berpartisipasi dalam pencegahan kejahatan siber keuangan. Seseorang akan lebih termotivasi untuk belajar terkait strategi pencegahan kejahatan siber keuangan, lebih termotivasi untuk menggunakan perangkat lunak perlindungan (antivirus), dan berpartisipasi dalam kegiatan yang bertujuan untuk mencegah kejahatan siber keuangan.

Persepsi ancaman yang tinggi juga dapat mendorong dukungan yang lebih kuat terhadap kebijakan keamanan siber keuangan yang diperlukan. Seseorang akan lebih termotivasi untuk mendukung upaya pemerintah atau lembaga terkait dalam mengimplementasikan kebijakan yang bertujuan untuk mengurangi risiko kejahatan siber keuangan. Hal tersebut dapat mencakup dukungan terhadap peningkatan keamanan ruang siber *(cyberspace)*, perumusan peraturan perundang-undangan yang lebih kuat terkait kejahatan siber, penegakan hukum yang lebih kuat, serta peningkatan hukuman bagi pelaku kejahatan siber keuangan.

4.5.5 Pengaruh Efikasi Diri Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Hipotesis kelima (H5) menguji hubungan antara efikasi diri dengan motivasi penghindaran kejahatan siber keuangan. Hipotesis 5 menyatakan bahwa efikasi diri berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa efikasi diri berpengaruh secara positif terhadap motivasi penghindaran kejahatan siber keuangan namun pengaruhnya tidak signifikan. Hal tersebut juga dapat diartikan bahwa efikasi diri tidak berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis kelima dalam penelitian ini **tidak diterima.**

Efikasi diri tidak berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan karena responden cenderung memiliki kepercayaan yang rendah terhadap kemampuan diri mereka untuk melindungi diri dari kejahatan. Mereka merasa tidak yakin dalam menghadapi situasi berisiko atau mengambil langkah-

langkah pencegahan yang diperlukan. Hal tersebut mengakibatkan berkurangnya motivasi mereka untuk melibatkan diri dalam upaya pencegahan kejahatan siber keuangan.

Penelitian ini sejalan dengan (Carpenter *et al.*, 2019) yang menunjukkan bahwa efikasi diri tidak berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan. Dalam penelitian ini, ketika efikasi diri tidak mempengaruhi motivasi penghindaran kejahatan siber keuangan, dapat diartikan bahwa seseorang kurang termotivasi untuk menggunakan perangkat lunak perlindungan (antivirus). Hal tersebut dikarenakan mereka tidak dapat melihat nilai atau manfaat dari perangkat lunak perlindungan (antivirus) tersebut karena mereka merasa tidak percaya diri dengan kemampuannya untuk mengoperasikan perangkat lunak tersebut.

Ketika efikasi diri tidak berpengaruh terhadap motivasi penghindaran kejahatan siber, implikasinya adalah kurangnya kesadaran akan ancaman kejahatan siber keuangan dan kurangnya kemampuan dalam menciptakan ruang siber yang aman sehingga dapat memperbesar peluang para pengguna perangkat elektronik untuk menjadi korban serangan kejahatan siber keuangan. Untuk mengatasi hal tersebut, diperlukan upaya untuk meningkatkan kesadaran, pengetahuan, keterampilan, dan dukungan terkait perlindungan perangkat lunak terhadap kejahatan siber keuangan. Pelatihan, peningkatan kesadaran akan pentingnya ruang siber yang aman, dan penciptaan lingkungan yang mendukung keamanan ruang siber sangat penting untuk meningkatkan motivasi seseorang dalam menghindari kejahatan siber keuangan dan menerapkan praktik keamanan yang lebih baik.

Selain itu, pengembang perangkat lunak perlindungan (antivirus) juga perlu menyediakan solusi keamanan yang efektif dan terpercaya. Hal tersebut termasuk mengembangkan perangkat lunak perlindungan yang kuat, perangkat pendeteksi kejahatan siber yang mudah digunakan oleh pengguna, dan fitur-fitur keamanan tambahan yang dapat membantu pengguna menerapkan langkah-langkah pencegahan yang diperlukan dengan mudah.

4.5.6 Pengaruh Efektivitas Perlindungan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Hipotesis keenam (H6) dalam penelitian ini menguji hubungan antara efektivitas perlindungan dengan motivasi penghindaran kejahatan siber keuangan. Hipotesis 6 menyatakan bahwa efektivitas perlindungan berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa efektivitas perlindungan memiliki pengaruh secara positif terhadap motivasi penghindaran kejahatan siber keuangan namun pengaruhnya tidak signifikan. Hal tersebut juga dapat diartikan bahwa efektivitas perlindungan berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis keenam dalam penelitian ini **diterima.**

Efektivitas perlindungan berpengaruh karena ketika pengguna perangkat elektronik menyadari bahwa antivirus yang mereka gunakan efektif dalam melindungi perangkat mereka, hal ini dapat mempengaruhi motivasi mereka untuk mengadopsi tindakan pencegahan yang proaktif. Penelitian ini sejalan dengan penelitian yang dilakukan oleh (Carpenter et al., 2019) yang membuktikan bahwa

efektivitas perlindungan berpengaruh positif terhadap motivasi penghindaran ancaman teknologi.

Efektivitas perlindungan yang tinggi juga dapat memengaruhi persepsi kontrol pengguna terhadap keamanan siber. Ketika pengguna merasa bahwa antivirus mereka mampu memberikan perlindungan, mereka merasa memiliki kendali dan pengaruh terhadap keamanan sistem mereka. Selain itu, efektivitas antivirus yang tinggi juga dapat memperkuat persepsi pengguna terhadap nilai dan manfaat dari tindakan pencegahan kejahatan siber keuangan. Ketika pengguna menyadari bahwa antivirus yang mereka gunakan mampu melindungi mereka dari ancaman, mereka mungkin lebih mungkin untuk melihat perlindungan diri sebagai suatu investasi yang berharga. Mereka menyadari bahwa tindakan pencegahan ini dapat membantu mengurangi risiko dan kerugian di masa depan, termasuk kerugian finansial, pencurian identitas, atau kerugian reputasi. Kesadaran akan manfaat ini dapat memotivasi pengguna untuk secara aktif mengadopsi strategi penghindaran kejahatan siber dan menjaga keamanan ruang siber mereka.

Implikasi dari hasil penelitian ini adalah pengembang perangkat lunak perlindungan (antivirus) perlu untuk terus meningkatkan efektivitas produk mereka. Hal tersebut melibatkan penelitian dan pengembangan yang berkelanjutan untuk mengatasi ancaman baru yang muncul dan meningkatkan kualitas perlindungan yang disediakan. Selain itu, penting bagi pengembang antivirus untuk berkomunikasi secara efektif dengan pengguna tentang manfaat dan keunggulan perlindungan yang diberikan, serta memberikan panduan dan sumber daya yang mendukung untuk membantu pengguna mengadopsi tindakan pencegahan yang

diperlukan. Dengan demikian, pengembang antivirus dapat memberikan kontribusi signifikan terhadap motivasi penghindaran kejahatan siber dan meningkatkan keamanan ruang siber secara keseluruhan.

4.5.7 Pengaruh *Safeguard Cost* Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Hipotesis ketujuh (H7) dalam penelitian ini menguji hubungan antara *safeguard cost* dengan motivasi penghindaran kejahatan siber keuangan. Hipotesis 7 menyatakan bahwa *safeguard cost* berpengaruh negatif terhadap motivasi penghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa *safeguard cost* memiliki pengaruh negatif terhadap motivasi penghindaran kejahatan siber keuangan namun pengaruhnya tidak signifikan. Hal tersebut dapat diartikan bahwa *safeguard cost* tidak berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis ketujuh dalam penelitian ini **tidak diterima**.

Hasil penelitian ini sejalan dengan penelitian oleh (Arachchilage et al., 2016) yang menunjukkan bahwa *safeguard cost* tidak berpengaruh terhadap motivasi penghindaran kejahatan *phishing* oleh mahasiswa ilmu komputer di UK. Dalam penelitian ini, *safeguard cost* tidak berpengaruh karena pekerja sektor keuangan cenderung tidak mempertimbangkan usaha yang perlu mereka keluarkan untuk memperoleh perangkat lunak perlindungan (antivirus). Situasi tersebut dapat terjadi karena pekerja sektor keuangan bekerja menggunakan perangkat yang telah disediakan oleh perusahaan. Oleh karena itu, pekerja sektor keuangan tidak perlu

memikirkan atau mempertimbangkan usaha yang harus dikeluarkan untuk memperoleh perangkat lunak perlindungan (antivirus).

Selain itu, setiap orang memiliki prioritas dan nilai-nilai yang berbeda dalam menggunakan sumber daya mereka. Jika mereka menganggap *safeguard cost* sebagai sesuatu yang tidak sebanding dengan manfaat atau nilai lain yang mereka anggap lebih penting, maka mereka tidak termotivasi untuk mengambil tindakan pencegahan yang melibatkan *safeguard cost* yang tinggi. Faktor lain yang dapat mempengaruhi motivasi penghindaran kejahatan adalah ketersediaan sumber daya. Apabila seseorang tidak memiliki sumber daya yang cukup untuk mengakses atau menerapkan tindakan perlindungan yang membutuhkan *effort* dan biaya yang tinggi, maka *safeguard cost* tidak akan mempengaruhi motivasi mereka. Mereka mungkin mencari alternatif pencegahan yang lebih terjangkau atau bergantung pada faktor-faktor lain seperti pengetahuan dan keterampilan untuk mengurangi risiko kejahatan siber.

Kurangnya pengaruh *safeguard cost* terhadap motivasi penghindaran kejahatan siber juga dapat menyebabkan seseorang mengabaikan pentingnya pencegahan kejahatan siber. Mereka mungkin cenderung memprioritaskan kebutuhan atau tujuan lain yang dianggap lebih penting daripada menginvestasikan sumber daya untuk tindakan perlindungan. Apabila *safeguard cost* tidak mempengaruhi motivasi penghindaran kejahatan, seseorang mungkin enggan untuk mengambil langkah-langkah perlindungan yang diperlukan. Hal ini dapat mengakibatkan rendahnya upaya pencegahan yang efektif, seperti *menginstall* perangkat lunak perlindungan. Selain itu, kurangnya motivasi seseorang untuk

melibatkan diri dalam tindakan perlindungan yang melibatkan *safeguard cost* dapat meningkatkan risiko kejahatan. Dalam situasi ini, mereka mungkin lebih rentan terhadap ancaman kejahatan karena tidak mengadopsi tindakan perlindungan yang memadai atau efektif.

Implikasinya terhadap perusahaan pengembang software perlindungan, apabila *safeguard cost* tidak berpengaruh terhadap motivasi penghindaran kejahatan, hal ini dapat menghambat inovasi dalam pengembangan solusi perlindungan yang lebih efektif dan terjangkau. Jika tidak ada insentif ekonomi untuk mengembangkan dan mengimplementasikan tindakan perlindungan yang mahal, maka kemungkinan besar pengembangan solusi perlindungan yang inovatif dan efisien akan terhambat.

4.5.8 Pengaruh Antisipasi Penyesalan Terhadap Motivasi Penghindaran Kejahatan Siber Keuangan

Hipotesis kedelapan (H8) dalam penelitian ini menguji hubungan antara antisipasi penyesalan dengan motivasi penghindaran kejahatan siber keuangan. Hipotesis 8 menyatakan bahwa antisipasi penyesalan berpengaruh positif terhadap motivasi penghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikasnsi statistik menunjukkan bahwa antisipasi penyesalan memiliki pengaruh secara positif dan signifikan terhadap motivasi penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis kedelapan dalam penelitian ini **diterima.**

Antisipasi penyesalan berpengaruh positif karena antisipasi penyesalan dapat membuat seseorang menjadi lebih sadar akan konsekuensi negatif yang mungkin terjadi jika mereka menjadi korban kejahatan siber keuangan. Hasil

penelitian ini sejalan dengan penelitian yang dilakukan oleh (Verkijika, 2019) yang menunjukkan bahwa antisipasi penyesalan berpengaruh positif terhadap motivasi penghindaran *phishing*. Mereka cenderung merasakan kekhawatiran dan penyesalan yang diantisipasi terkait dengan dampak yang merugikan, seperti kerugian finansial. Kesadaran akan konsekuensi ini dapat memotivasi mereka untuk menghindari perilaku yang berpotensi menyebabkan penyesalan di masa depan.

Antisipasi penyesalan juga dapat meningkatkan persepsi risiko seseorang terhadap kejahatan. Mereka mungkin lebih cenderung memperhatikan potensi risiko dan bahaya yang terkait dengan kejahatan siber, dan mempertimbangkan secara serius dampak negatif yang mungkin terjadi. Hal ini dapat meningkatkan motivasi mereka untuk mengambil langkah-langkah pencegahan yang diperlukan untuk menghindari risiko tersebut.

Implikasi dari penelitian ini adalah tingkat antisipasi penyesalan yang tinggi menyebabkan seseorang cenderung mengadopsi strategi penghindaran yang proaktif seperti menginstal perangkat lunak perlindungan, menggunakan kata sandi yang kuat, rutin memperbarui perangkat lunak, dan/atau menyetujui kebijakan keamanan yang disarankan. Mereka menyadari bahwa tindakan pencegahan ini dapat membantu mengurangi risiko dan menghindari penyesalan di masa depan.

4.5.9 Pengaruh Motivasi Penghindaran Kejahatan Siber Keuangan Terhadap Perilaku Penghindaran Kejahatan Siber Keuangan

Hipotesis kesembilan (H9) dalam penelitian ini menguji hubungan antara motivasi penghindaran kejahatan siber keuangan dan perilaku penghindaran kejahatan siber keuangan. Hipotesis 9 menyatakan bahwa motivasi penghindaran

kejahatan siber keuangan berpengaruh positif terhadap perilaku peghindaran kejahatan siber keuangan. Hasil analisis koefisien jalur dan signifikansi statistik menunjukkan bahwa motivasi penghindaran kejahatan siber keuangan memiliki pengaruh secara positif dan signifikan terhadap perilaku penghindaran kejahatan siber keuangan. Oleh karena itu, hipotesis kesembilan dalam penelitian ini **diterima.**

Motivasi penghindaran kejahatan siber keuangan berpengaruh positif terhadap perilaku penghindaran kejahatan siber keuangan karena seseorang yang memiliki motivasi penghindaran kejahatan yang tinggi cenderung mengadopsi tindakan pencegahan untuk melindungi diri mereka dari risiko kejahatan. Hasil peneltitian ini sejalan dengan Gillam dan Foster (2021); Butler (2020); dan Verkijika (2019) yang menunjukkan bahwa motivasi penghindaran kejahatan siber berpengaruh terhadap perilaku penghindaran kejahatan siber. Seseornag yang memiliki motivasi untuk menghindari kejahatan siebr cenderung akan menginstal perangkat lunak perlindungan, menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, atau menghindari perilaku yang berisiko di ruang siber *(cyberspace)*. Motivasi ini mendorong mereka untuk bertindak proaktif dalam mengurangi risiko dan menjaga keamanan ruang siber.

Motivasi penghindaran kejahatan yang tinggi juga dapat meningkatkan tingkat kewaspadaan seseorang terhadap potensi ancaman kejahatan siber. Mereka mungkin lebih peka terhadap tanda-tanda yang mencurigakan atau situasi berpotensi berbahaya, sehingga memungkinkan mereka untuk menghindari atau mengurangi interaksi dengan risiko kejahatan siber.

Selain itu, motivasi penghindaran kejahatan dapat mendorong seseorang untuk meningkatkan pengetahuan dan kesadaran mereka tentang jenis-jenis kejahatan siber keuangan yang ada dan cara-cara untuk menghindarinya. Mereka mungkin akan lebih proaktif dalam mengikuti pelatihan praktik keamanan terbaru, berpartisipasi dalam program edukasi kejahatan siber keuangan, atau mencari referensi yang dapat membantu mereka untuk mempelajari, mengidentifikasi, dan menghindari ancaman kejahatan siber keuangan.

Dengan adanya motivasi penghindaran kejahatan siber keuangan yang kuat dapat memicu seseorang untuk terbiasa berperilaku aman. Seseorang yang memiliki motivasi penghindaran kejahatan siber keuangan cenderung secara konsisten akan mengadopsi langkah-langkah penghindaran kejahatan siber dalam kehidupan sehari-hari mereka, sehingga mereka dapat meningkatkan tingkat keamanan siber secara keseluruhan.

BAB 5

PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk menguji secara empiris pengaruh Persepsi Kerentanan terhadap Persepsi Ancaman, Persepsi Keparahan terhadap Persepsi Ancaman, Interaksi antara Persepsi Kerentanan dan Persepsi Keparahan terhadap Persepsi Ancaman, Persepsi Ancaman terhadap Motivasi Penghindaran Kejahatan Siber Keuangan, Efikasi Diri terhadap Motivasi Penghindaran Kejahatan Siber Keuangan, Efektivitas Perlindungan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan, *Safeguard Cost* terhadap Motivasi Penghindaran Kejahatan Siber Keuangan, Antisipasi Penyesalan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan, dan Motivasi Penghindaran Kejahatan Siber Keuangan terhadap Perilaku Penghindaran Kejahatan Siber Keuangan. Pengambilan sampel dalam penelitian ini menggunakan metode *convenience sampling*. Sampel dalam penelitian ini sebanyak 180 pekerja sektor keuangan di Indonesia yang menggunakan perangkat elektronik dalam bekerja.

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa:

1. Persepsi Kerentanan berpengaruh positif signifikan terhadap Persepsi Ancaman. Ketika seseorang merasa rentan terhadap serangan kejahatan siber keuangan, mereka cenderung akan lebih peka dengan risiko atau bahaya yang mungkin akan terjadi. Ketika seseorang meyakini bahwa banyak risiko yang

dapat terjadi di masa depan, untuk menghindarinya mereka akan meningkatkan persepsi ancaman yang mereka yakini.

2. Persepsi Keparahan berpengaruh positif signifikan terhadap Persepsi Ancaman. Ketika seseorang menganggap bahwa kejahatan siber keuangan akan mengakibatkan ancaman kejahatan siber keuangan merupakan salah satu hal yang serius, maka ia akan merasa terancam.
3. Tidak terdapat pengaruh interaksi antara Persepsi Kerentanan dan Persepsi Keparahan terhadap Persepsi Ancaman. Hal tersebut dikarenakan ketika seseorang berpikir bahwa mereka rentan terhadap serangan kejahatan siber keuangan, disaat yang sama mereka percaya bahwa kerentanan tersebut tidak akan mengakibatkan suatu hal yang parah.
4. Persepsi Ancaman berpengaruh positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Persepsi ancaman yang tinggi dapat meningkatkan tingkat kewaspadaan pekerja sektor keuangan terhadap potensi kejahatan siber keuangan. Para pekerja sektor keuangan akan lebih waspada sehingga mereka akan termotivasi untuk melakukan tindakan penghindaran kejahatan siber keuangan.
5. Efikasi Diri tidak berpengaruh terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Hal tersebut dikarenakan mereka tidak dapat melihat nilai atau manfaat dari perangkat lunak perlindungan (antivirus) tersebut karena mereka merasa tidak percaya diri dengan kemampuannya untuk mengoperasikan perangkat lunak tersebut. Ketika efikasi diri tidak berpengaruh terhadap motivasi penghindaran kejahatan siber, implikasinya

adalah kurangnya kesadaran akan ancaman kejahatan siber keuangan dan kurangnya kemampuan dalam menciptakan ruang siber yang aman sehingga dapat memperbesar peluang para pengguna perangkat elektronik untuk menjadi korban serangan kejahatan siber keuangan.

6. Efektivitas Perlindungan berpengaruh positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Ketika pekerja sektor keuangan menyadari bahwa antivirus yang mereka gunakan efektif dalam melindungi perangkat mereka, hal ini dapat meningkatkan motivasi mereka untuk mengadopsi tindakan pencegahan yang proaktif.
7. *Safeguard Cost* tidak berpengaruh terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Dalam penelitian ini, pekerja sektor keuangan cenderung tidak mempertimbangkan usaha yang perlu mereka keluarkan untuk memperoleh perangkat lunak perlindungan (antivirus). Situasi tersebut dapat terjadi karena pekerja sektor keuangan bekerja menggunakan perangkat yang telah disediakan oleh perusahaan. Oleh karena itu, pekerja sektor keuangan tidak perlu memikirkan atau mempertimbangkan usaha yang harus dikeluarkan untuk memperoleh perangkat lunak perlindungan (antivirus).
8. Antisipasi Penyesalan berpengaruh positif signifikan terhadap Motivasi Penghindaran Kejahatan Siber Keuangan. Antisipasi penyesalan dapat membuat seseorang menjadi lebih sadar akan konsekuensi negatif yang mungkin terjadi jika mereka menjadi korban kejahatan siber keuangan. Tingkat antisipasi penyesalan yang tinggi akan menyebabkan seseorang cenderung mengadopsi strategi penghindaran yang proaktif seperti menginstal perangkat

lunak perlindungan, menggunakan kata sandi yang kuat, rutin memperbarui perangkat lunak, dan/atau menyetujui kebijakan keamanan yang disarankan. Mereka menyadari bahwa tindakan pencegahan tersebut dapat membantu mengurangi risiko dan menghindari penyesalan di masa depan.

9. Motivasi Penghindaran Kejahatan Siber Keuangan berpengaruh positif signifikan terhadap Perilaku Penghindaran Kejahatan Siber Keuangan. Seseorang yang memiliki motivasi penghindaran kejahatan siber keuangan cenderung secara konsisten akan mengadopsi langkah-langkah penghindaran kejahatan siber dalam kehidupan sehari-hari mereka, sehingga mereka dapat meningkatkan tingkat keamanan siber secara keseluruhan.

5.2 Kontribusi dan Implikasi

5.2.1 Kontribusi

Studi ini menggali sejumlah temuan menarik yang akan memberikan kontribusi teoritis pada literatur yang telah ada sebelumnya. Penelitian ini berkontribusi pada literatur perilaku penghindaran kejahatan siber keuangan di Indonesia. Penelitian ini diharapkan menjadi acuan atau sumber referensi yang relevan bagi akademisi yang akan melaksanakan penelitian selanjutnya dengan topik terkait.

5.2.2 Implikasi

Dari hasil penelitian maka terdapat beberapa implikasi yang dapat disimpulkan yaitu:

1. Implikasi bagi pemerintah atau regulator terkait kemanan siber yaitu regulator dapat mempertimbangkan faktor-faktor yang mempengaruhi perilaku

penghindaran kejahatan siber keuangan di Indonesia dalam merumuskan atau menetapkan peraturan yang terkait. Selain itu, persepsi ancaman yang berpengaruh terhadap motivasi penghindaran kejahatan siber keuangan dapat memicu pemerintah untuk segera bertindak cepat untuk merumuskan atau menetapkan kebijakan yang lebih baik terkait kemanan siber agar dapat mengurangi persepsi ancaman kejahatan siber keuangan yang diyakini oleh masyarakat.

2. Implikasi bagi pengembang sistem atau perangkat lunak perlindungan (antivirus) yaitu, para pengembang dapat mempertimbangkan faktor efikasi diri, *safeguard cost*¸ dan efektivitas perlindungan dalam meningkatkan inovasi penelitian dan pengembangan produk. Ketika inovasi yang dihasilkan oleh pengembang perangkat lunak dapat sesuai dengan kondisi yang dibutuhkan oleh masyarakat, maka inovasi tersebut akan membantu meningkatkan motivasi penghindaran kejahatan siber keuangan. Dengan meningkatnya motivasi penghindaran kejahatan siber keuangan, maka seiring berjalannya waktu akan meningkatkan keamanan ruang siber secara keseluruhan.
3. Implikasi bagi pengguna teknologi informasi yaitu hasil penelitian ini dapat digunakan oleh pengguna teknologi informasi sebagai pertimbangan pengambilan keputusan dalam hal merespon atau menghindari kejahatan siber keuangan.

5.3 Keterbatasan Penelitian dan Saran

5.3.1 Keterbatasan

Dalam penelitian ini memiliki beberapa keterbatasan yang dapat memepngaruhi hasil penelitian yang dicapai. Berikut ini keterbatasan pada penelitian ini:

1. Pada saat pengisian kuesioner, tidak semua responden didampingi sehingga terdapat kemungkinan jika responden kurang memahami maksud dari tiap item pertanyaan yang diajukan.
2. Pada variabel *safeguard cost*, dari 4 item indikator pengukuran hanya 2 item indikator yang dapat digunakan. Hal tersebut bisa jadi mengakibatkan perubahan hasil dari pengujian variabel yang dilakukan.

5.3.2 Saran

Dalam penelitian ini terdapat beberapa saran untuk penelitian selanjutnya yaitu:

1. Penelitian selanjurnya diharapkan dapat mempertimbangkan variabel-variabel lain yang dapat mempengaruhi perilaku penghindaran kejahatan siber keuangan.
2. Penelitian selanjutnya diharapkan dapat melakukan penelitian pada sektor industri lain yang juga termasuk dalam korban kejahatan siber keuangan dengan persentase terbesar.

DAFTAR PUSTAKA

Abdillah, W., & Jogiyanto. (2015). *Partial Least Square (PLS): Alternatif Structural Equation Modelling (SEM) dalam Penelitian Bisnis* (D. Prabantini, Ed.; 1st ed.). Penerbit ANDI.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/https://doi.org/10.1016/j.chb.2016.02.065

Baker, A. W., Keshaviah, A., Horenstein, A., Goetter, E. M., Mauro, C., Reynolds, C. F., Zisook, S., Katherine Shear, M., & Simon, N. M. (2016). The Role of Avoidance in Complicated Grief: A Detailed Examination of the Grief-Related Avoidance Questionnaire (GRAQ) in a Large Sample of Individuals with Complicated Grief. *Journal of Loss and Trauma*, *21*(6), 533–547. https://doi.org/10.1080/15325024.2016.1157412

Bandura, A. (1986). *Social Foundations of Thought and Action. A Social Cognitive Theory*. Prentice Hall.

Baral, G., Asanka, N., & Arachchilage, G. (n.d.). *Building Confidence not to be Phished through a Gamified Approach: Conceptualising User's Self-Efficacy in Phishing Threat Avoidance Behaviour*.

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers and Security*, *106*. https://doi.org/10.1016/j.cose.2021.102278

Bell, D. E. (1982). Regret in Decision Making Under Uncertainty. *Operations Research*, *30*(5), 961–981. https://doi.org/doi:10.1287/opre.30.5.961

Bennett, M., & Galpert, L. (1992). Complex Belief-Desire Reasoning in Children. *Social Development*, *1*(3), 201–210. https://doi.org/https://doi.org/10.1111/j.1467-9507.1992.tb00124.x

Braverman, J., & Frost, J. H. (2012). Matching The Graphical Display of Data to Avoidance Versus Approach Motivation Increases Outcome Expectancies. *The Journal of Social Psychology*, *152*(2), 228–245. https://doi.org/https://doi.org/10.1080/00224545.2011.598583

Brewer, N. T., DeFrank, J. T., & Gilkey, M. B. (2016). Anticipated regret and health behavior: A meta-analysis. *Health Psychology*, *35*(11), 1264–1275. https://doi.org/10.1037/hea0000294

Butler, R. (2020). A Systematic Literature Review of The Factors Affecting Smartphone User Threat Avoidance Behaviour. In *Information and Computer*

Security (Vol. 28, Issue 4, pp. 555–574). Emerald Group Holdings Ltd. https://doi.org/10.1108/ICS-01-2020-0016

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 380–407. https://doi.org/10.17705/1CAIS.04422

Djatsa, F. (2020). Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations. *Journal of Information Security*, *11*(01), 19–45. https://doi.org/10.4236/jis.2020.111002

Elliot, A. J., Eder, A. B., & Harmon-Jones, E. (2013). Approach-Avoidance Motivation and Emotion: Convergence and Divergence. *Emotion Review*, *5*(3), 308–311. https://doi.org/10.1177/1754073913477517

Fishburn, P. C. (1982). The Foundations of Expected Utility. In *Theory & Decision Library*. https://doi.org/ISBN 90-277-1420-7

Ghozali, I., & Latan, H. (2015). *Partial Least Squares Konsep, Teknik Dan Aplikasi Menggunakan Smart PLS 3.0 Untuk Penelitian Empiris* (2nd ed.). Badan Penerbit UNDIP.

Gillam, A. R., & Foster, W. T. (2020a). Factors Affecting Risky Cybersecurity Behaviors by U.S. Workers: An Exploratory Study. *Computers in Human Behavior*, *108*, 1–12. https://doi.org/10.1016/j.chb.2020.106319

Gillam, A. R., & Foster, W. T. (2020b). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, *108*. https://doi.org/10.1016/j.chb.2020.106319

Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security* (1st ed.). Springer International Publishing.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Ibm. (n.d.). *Analysis of cyber attack and incident data from IBM's worldwide security operations IBM Global Technology Services Managed Security Services Research Report*.

IBM. (2022). *X-Force Threat Intelligence Index 2022 Full Report*.

Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. *Business Management Dynamics*, *5*(11), 16–39. www.bmdynamics.com

Kasmaei, P., Shokravi, F. A., Hidarnia, A., Hajizadeh, E., Atrkar-Roushan, Z., Shirazi, K. K., & Montazeri, A. (2014). Brushing Behavior Among Young Adolescents: Does Perceived Severity Matter. *BMC Public Health*, *14*(8). https://doi.org/10.1186/1471-2458-14-8

Klein, P., Nir-Gal, O., & Darom, E. (2000). The use of computers in kindergarten with or without adult mediation: Effects on children's cognitive performance and behavior. *Computers in Human Behavior*, *16*(6), 591–608. https://doi.org/https://doi.org/10.1016/S0747-5632(00)00027-3

Levkovich, I., & Shinan-Altman, S. (2021). The impact of gender on emotional reactions, perceived susceptibility and perceived knowledge about COVID-19 among the Israeli public. *International Health*, *13*(6), 555–561. https://doi.org/10.1093/inthealth/ihaa101

Liang, H., & Xue, Y. (2009a). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly: Management Information Systems*, *33*(1), 71–90. https://doi.org/10.2307/20650279

Liang, H., & Xue, Y. (2009b). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly: Management Information Systems*, *33*(1), 71–90. https://doi.org/10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Loomes, G., & Sugden, R. (1982). Regret Theory: An Alternative Theory of Rational Choice Under Uncertainty. *The Economic Journal*, *92*(368), 805–824. https://doi.org/https://doi.org/10.2307/2232669

Mark, M. S., Borda, O., Stroman, J., Member, C., & Wilson, T. C. (2021). *An Analysis of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study*.

Maskun. (2014). *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (2nd ed.). Kencana.

NCSI. (2022). *National Cyber Security Index - Indonesia*. *9*, 2–3.

Oz, B., Ozkan, T., & Lajunen, T. (2013). An investigation of professional drivers: Organizational safety climate, driver behaviours and performance. *Transportation Research*, *16*, 81–91. https://doi.org/https://doi.org/10.1016/j.trf.2012.08.005

PwC. (2022). *PwC's Global Economic Crime and Fraud Survey 2022*.

Saidi, K., & Prayudi, Y. (2021). *Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT)*.

Schindler, P. S. (2019). *Business Research Methods*. McGraw-Hill Education. https://doi.org/9813158581; 9789813158580

Sheynin, J., Beck, K. D., Servatius, R. J., & Myers, C. E. (2014). Acquisition and Extinction of Human Avoidance Behavior: Attenuating Effect of Safety Signals and Associations With Anxiety Vulnerabilities. *Frontiers in Behavioral Neuroscience*, *8*(SEP), 1–11. https://doi.org/10.3389/fnbeh.2014.00323

Shih, E., & Schau, H. J. (2011). To Justify or Not to Justify: The Role of Anticipated Regret on Consumers' Decisions to Upgrade Technological Innovations. *Journal of Retailing*, *87*(2), 242–251. https://doi.org/https://doi.org/10.1016/j.jretai.2011.01.006

Sukamulja, S., Meilita, A. Y. N., & Senoputri, D. (2019). Regret Aversion Bias, Mental Accounting, Overconfidence, and Risk Perception in Investment Decision Making on Generation Y Workers in Yogyakarta. *International Journal of Economics and Management Studies*, *6*(7), 102–110. https://doi.org/10.14445/23939125/ijems-v6i7p116

Sylvester, F. L. (2022). Mobile Device Users' Susceptibility to Phishing Attacks. *International Journal of Computer Science and Information Technology*, *14*(1), 1–18. https://doi.org/10.5121/ijcsit.2022.14101

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2). https://doi.org/10.1016/j.giq.2021.101572

The World Bank and the United Nations. (2017). *Combatting Cybercrime*.

Triwibowo, C. (2015). *Pengantar Dasar Ilmu Kesehatan Masyarakat*. Nuha Medika.

Verkijika, S. F. (2019). If You Know What to Do, Will You Take Action to Avoid Mobile Phishing Attacks: Self-Efficacy, Anticipated Regret, and Gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/https://doi.org/10.1016/j.chb.2019.07.034

We Are Social Hootsuite. (2022). *The Global State of Digital 2022*.

Xiling, H., Yuli, Z., Yiran, L., & Yan-ping, P. (2018). A Theoretical Framework for Counterfactual Thinking in The Context of Entrepreneurial Failure. *Foreign Economics and Management*, *40*, 3–15. https://doi.org/10.16538/j.cnki.fem.2018.04.001

LAMPIRAN

Lampiran 1.

Kuesioner Penelitian

Determinan Perilaku Penghindaran Kejahatan Siber Keuangan oleh Pekerja Sektor Keuangan di Indonesia

Assalamualaikum Wr. Wb.

Yth. Bapak/Ibu/Saudara/i responden

di Tempat

Perkenalkan, saya Hanifah Zahra mahasiswa program studi Magister Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, Yogyakarta. Saat ini saya sedang melaksanakan penelitian untuk memenuhi tugas akhir sebagai syarat kelulusan S-2 Akuntansi dengan topik penelitian "Perilaku Penghindaran Kejahatan Siber Keuangan". Oleh sebab itu, saya mohon kesediaan Anda untuk mengisi kuesioner ini.

Seluruh jawaban yang Anda berikan akan saya jaga kerahasiaannya dan hanya digunakan untuk kepentingan penelitian.

Atas perhatian dan kesediaan untuk berpartisipasi dalam penelitian ini, saya ucapkan terima kasih.
Wassalamualaikum Wr. Wb.

Dengan hormat,
Hanifah Zahra

A. Pengertian Kejahatan Siber Keuangan

Kejahatan siber keuangan merupakan kejahatan yang dilakukan dalam sistem berbasis perangkat elektronik atau jaringan internet yang menimbulkan kerugian secara keuangan. Pelaku kejahatan siber keuangan umumnya mencuri data pribadi milik korban melalui skema penipuan atau menggunakan *malware* (virus) yang disisipkan pada perangkat elektronik milik korban.

Bentuk kejahatan siber keuangan dapat berupa:

a. Kejahatan *Carding* : Kejahatan siber berupa pembobolan data kartu kredit dan pelaku melakukan transaksi menggunakan data kartu kredit milik korban.

b. Pemerasan Siber : Kejahatan siber dengan modus pelaku akan meminta uang sebagai tebusan atas data penting yang telah dicuri.

c. Serangan *Adware* : Kejahatan siber berupa iklan/pemberitahuan yang muncul tanpa izin atau email *spam* yang berisikan hadiah atau penawaran uang dalam jumlah yang tidak realistis.

d. Penipuan OTP : Kejahatan siber berupa pesan/telepon berisi permintaan OTP (*one-time password*) untuk verifikasi aplikasi atau *website*. Pada umumnya, pelaku akan menyamar menjadi pihak bank atau instansi tertentu.

e. Penipuan Link Palsu : Kejahatan siber dimana pelaku mengirimkan link palsu kepada korban dengan tujuan mencuri data rekening milik orang yang mengakses tautan tersebut. (Contoh: kasus link palsu resi paket dan link palsu persetujuan perubahan kebijakan bank).

f. Penipuan Pesan Berisi APK : Kejahatan siber berupa pesan berisi APK (aplikasi android) yang terinfeksi *malware.* Ketika aplikasi tersebut terpasang pada perangkat elektronik milik korban, maka pelaku dapat mencuri data penting milik korban. (Contoh: pesan berisi APK yang berkedok undangan pernikahan digital).

Kejahatan siber keuangan adalah segala bentuk kejahatan dengan menggunakan perangkat elektronik dan jaringan internet yang target utamanya merupakan uang milik korban. Kejahatan siber keuangan umumnya akan menyalahgunakan identitas orang lain seperti nama, nama ibu kandung, nomor telepon, nomor identitas diri, dan kata sandi guna mengambil keuntungan finansial seperti mengambil pinjaman, masuk ke rekening bank atau akun keuangan *online*, atau mengklaim asuransi. Selain itu, kejahatan siber keuangan tidak hanya menyasar pada suatu individu namun juga dapat menyerang suatu perusahaan dengan tujuan mencuri data-data penting milik perusahaan.

B. Identitas Responden

Pada bagian ini, responden dimohon untuk mengisi identitas diri.

Nama : _____ (boleh disamarkan)

Gender : □ Laki-laki □ Perempuan

Usia : □ < 20 tahun □ 40-49 tahun
□ 20-29 tahun □ 50-59 tahun
□ 30-39 tahun □ > 59 tahun

Apakah Anda bekerja pada industri sektor keuangan?

□ Ya □ Tidak

Kategori Industri Keuangan*) : □ Perbankan □ Lembaga Pembiayaan (*leasing*, anjak piutang, dsb)
□ Asuransi
□ Perusahaan Sekuritas □ Pegadaian
□ Koperasi Simpan Pinjam □ Lainnya: _____

Nama Perusahaan*) : _____ (boleh disamarkan)

Wilayah Tempat Bekerja*) : _____

Lama Bekerja*) : □ 1-3 tahun □ 7-10 tahun
□ 4-7 tahun □ > 10 tahun

Bidang Profesi*) : □ Administrasi □ HRD
□ Pemasaran & Penjualan □ *General Affair*
□ Akuntansi & Keuangan □ Lainnya:_____
□ Teknologi Informasi

Apakah Anda menggunakan perangkat elektronik (komputer/laptop/tablet/*handphone*) yang terhubung dengan jaringan internet dalam bekerja?

□ Ya □ Tidak

Apakah Anda pernah menjadi korban serangan siber keuangan?

 Ya Tidak

Apabila pernah mendapat serangan kejahatan siber keuangan, bentuk kejahatan seperti apa yang pernah Anda alami?

 Kejahatan *Carding*
 Pemerasan Siber
 Serangan *Adware*
 Penipuan OTP
 Penipuan Link Palsu
 Penipuan Pesan Berisi APK
 Lainnya: _____

C. Indikator Variabel

Pada bagian ini, Anda diminta untuk mengisi jawaban dengan memilih salah satu dari pilihan yang tersedia. Beri tanda centang pada kolom yang dipilih.

1 : Sangat Tidak Setuju
2 : Tidak Setuju
3 : Agak Tidak Setuju
4 : Agak Setuju
5 : Setuju
6 : Sangat Setuju

A	Persepsi Kerentanan	1	2	3	4	5	6
1.	Sangat mungkin bagi perangkat elektronik saya untuk menjadi target kejahatan siber keuangan di masa yang akan datang.						
2.	Peluang saya untuk menjadi korban kejahatan siber keuangan melalui perangkat elektronik cukup besar.						
3.	Terdapat kemungkinan besar bahwa perangkat elektronik saya berisi atau terinfeksi *malware* (virus) yang dapat mencuri data pribadi saya.						

B	Persepsi Keparahan	1	2	3	4	5	6
1.	Pelaku kejahatan siber keuangan dapat mengumpulkan data pribadi dari perangkat elektronik milik saya tanpa sepengetahuan saya.						
2.	Data pribadi saya yang dikumpulkan oleh pelaku kejahatan siber keuangan dari perangkat elektronik milik saya dapat disalahgunakan.						
3.	Serangan kejahatan siber keuangan dapat memperlambat kinerja perangkat elektronik dan koneksi jaringan internet saya.						

C	Persepsi Ancaman	1	2	3	4	5	6
1.	Serangan kejahatan siber keuangan pada perangkat elektronik dapat menimbulkan ancaman bagi saya.						
2.	Masalah yang disebabkan oleh serangan kejahatan siber keuangan pada perangkat elektronik berbahaya bagi saya.						
3.	Kejahatan siber keuangan berbahaya bagi perangkat elektronik dan jaringan internet saya.						
4.	Saya tidak dapat membayangkan apabila saya menjadi korban kejahatan siber keuangan yang menyerang perangkat elektronik milik saya.						

D	Efikasi Diri	1	2	3	4	5	6
1.	Saya yakin bahwa tanpa bantuan orang lain, saya dapat memperoleh pengetahuan terkait ancaman kejahatan siber keuangan yang dapat menyerang perangkat elektronik saya.						
2.	Saya merasa yakin dengan kemampuan saya untuk mendeteksi serangan kejahatan siber keuangan di perangkat elektronik saya.						
3.	Saya merasa yakin dengan kemampuan saya untuk mendeteksi aplikasi/*software* pada perangkat elektronik saya yang bukan berasal dari sumber terpercaya.						
4	Saya yakin saya memiliki kemampuan untuk mengidentifikasi SMS/email yang mengandung						

D	Efikasi Diri	1	2	3	4	5	6
	tautan/*link* berbahaya pada perangkat elektronik saya.						

E	Efektivitas Perlindungan	1	2	3	4	5	6
1.	*Software* perlindungan (antivirus) akan berguna untuk mendeteksi dan menghapus serangan kejahatan siber keuangan pada perangkat elektronik saya.						
2.	*Software* perlindungan (antivirus) dapat meningkatkan kinerja saya untuk melindungi perangkat elektronik saya dari serangan kejahatan siber keuangan.						
3.	*Software* perlindungan (antivirus) dapat meningkatkan efektivitas saya dalam menemukan dan menghapus serangan kejahatan siber keuangan di perangkat elektronik saya.						

F	***Safeguard Cost***	1	2	3	4	5	6
1.	Proses untuk memperoleh *software* perlindungan (antivirus) pada perangkat elektronik akan membutuhkan banyak waktu & tenaga, karena proses untuk memperoleh *software* tersebut tidak mudah.						
2.	Proses instalasi *software* perlindungan (antivirus) pada perangkat elektronik akan membutuhkan banyak waktu & tenaga, karena proses instalasi *software* tersebut tidak mudah.						

F	*Safeguard Cost*	1	2	3	4	5	6
3.	Adanya *software* perlindungan (antivirus) pada perangkat elektronik akan mengganggu kenyamanan saya karena *software* tersebut dapat menimbulkan masalah pada perangkat elektronik saya.						
4.	Berlangganan *software* perlindungan (antivirus) pada perangkat elektronik merupakan salah satu wujud pemborosan karena biaya berlangganan *software* tersebut tidak murah.						

G	Antisipasi Penyesalan	1	2	3	4	5	6
1.	Saya akan menyesal apabila gagal mengambil langkah yang diperlukan untuk melindungi perangkat elektronik saya dari serangan kejahatan siber keuangan.						
2.	Saya akan menyesal apabila saya memasang *software* yang berasal dari sumber tidak terpercaya pada perangkat elektronik saya.						
3.	Saya akan menyesal apabila saya membuka tautan dari SMS/e-mail yang mengandung virus di perangkat elektronik saya.						

H	Motivasi Penghindaran	1	2	3	4	5	6
1.	Saya termotivasi memperoleh pengetahuan terkait kejahatan siber keuangan untuk menghindari kejahatan siber keuangan yang menyerang perangkat elektronik milik saya.						
2.	Saya termotivasi menggunakan *software* perlindungan (antivirus) untuk menghindari serangan kejahatan siber keuangan pada perangkat elektronik milik saya.						
3.	Saya termotivasi untuk berbagi pengetahuan terkait kejahatan siber keuangan kepada orang lain agar mereka tidak menjadi korban kejahatan siber keuangan.						
4.	Saya termotivasi mengajak orang lain untuk menggunakan *software* perlindungan (antivirus) pada perangkat elektronik untuk menghindari serangan kejahatan siber keuangan.						

I	Perilaku Penghindaran Kejahatan Siber	1	2	3	4	5	6
1.	Saya selalu memverifikasi seluruh email berasal dari sumber terpercaya sebelum membuka lampiran atau tautan apapun di perangkat elektronik saya.						
2.	Saya selalu memverifikasi keaslian pesan sebelum membuka tautan dari SMS atau *messaging platform* pada perangkat elektronik saya. (Misal:						

I	Perilaku Penghindaran Kejahatan Siber	1	2	3	4	5	6
	WhatsApp, Line, Facebook Messenger).						
3.	Saya hanya mengizinkan notifikasi (pemberitahuan) dari situs atau *software* terpercaya pada perangkat elektronik saya.						
4.	Seluruh *software* yang terpasang pada perangkat elektronik saya selalu berasal dari sumber terpercaya.						
5.	Saya selalu memperbarui sistem operasi & seluruh *software* yang terpasang dalam perangkat elektronik secara berkala segera setelah pembaruan tersedia.						
6.	Saya menjalankan *software* perlindungan perangkat elektronik (antivirus) secara teratur untuk menghindari serangan kejahatan siber keuangan di perangkat elektronik saya.						

Lampiran 2.

Tabulasi Data

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
1	6	4	4	2	5	2	4	4	2	2	5	6	6	6	2	2	4	5	2	2	5	5	5	5	4	4	5	5	2	5	2	5
2	2	2	2	5	5	3	3	4	4	3	3	4	4	4	2	5	5	5	2	5	5	5	3	5	4	4	5	5	4	5	5	5
3	3	3	4	4	4	3	3	3	3	4	3	3	3	4	4	4	4	3	3	4	4	4	4	3	4	3	5	5	5	5	3	3
4	5	5	5	5	5	4	5	5	5	5	4	2	2	2	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	4	5	5	5	5	4	2	2	2	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
6	5	3	3	5	5	2	5	5	2	4	2	2	2	4	3	3	3	2	2	5	5	5	5	4	5	4	5	5	5	3	3	5
7	5	5	5	5	5	5	5	5	5	4	3	3	3	3	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
8	3	3	3	5	5	5	5	5	5	5	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
9	5	4	5	5	5	6	5	5	6	5	1	2	2	1	5	6	5	5	5	5	6	6	6	6	6	5	5	5	5	5	5	5
10	5	5	6	6	6	5	6	6	6	6	2	1	1	2	5	6	6	5	5	6	6	5	6	6	6	6	5	6	6	5	5	5
11	6	5	5	6	6	5	6	6	5	6	2	2	2	2	5	5	5	4	4	5	5	6	5	5	5	5	5	5	5	5	5	5
12	6	5	5	6	6	5	6	6	4	4	3	2	2	2	5	5	5	4	4	5	5	6	6	6	6	6	5	6	5	6	5	5
13	5	5	5	5	5	5	5	5	5	5	2	3	3	2	5	5	5	5	4	5	5	5	5	5	5	5	5	4	5	4	4	4
14	6	6	6	6	6	5	6	6	6	6	2	2	2	2	5	5	5	5	4	6	5	5	5	4	4	4	6	6	6	6	6	6
15	6	5	5	6	6	6	5	6	5	4	1	2	2	5	6	6	6	5	4	5	6	6	6	5	5	4	6	6	6	6	6	6
16	6	5	5	5	6	6	6	6	6	6	4	4	5	5	4	4	4	4	5	5	6	6	6	6	6	6	6	6	6	5	6	5
17	6	5	6	5	6	6	6	6	6	6	4	4	5	5	5	5	5	4	5	5	6	6	6	6	6	6	6	6	6	5	6	5
18	6	4	4	5	6	5	6	6	6	6	3	3	4	4	4	4	4	5	5	5	6	6	6	6	6	6	6	6	6	5	6	5

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
19	6	4	4	5	6	5	6	6	6	6	3	3	3	4	4	4	4	5	5	5	6	6	6	6	6	6	6	6	5	4	5	5
20	6	5	5	5	6	2	6	6	4	6	2	4	4	5	4	4	4	5	4	6	6	6	6	4	6	4	4	6	4	5	5	4
21	6	6	6	6	6	6	6	6	6	3	4	3	5	6	4	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6
22	6	4	6	6	6	5	6	6	4	5	4	4	3	4	4	4	4	4	4	5	5	5	6	5	6	4	5	5	5	5	4	4
23	5	3	4	5	5	5	5	5	5	3	2	4	3	2	4	5	5	1	1	4	4	4	5	5	5	5	5	5	5	5	5	5
24	5	2	5	5	5	5	5	5	6	6	1	1	1	1	5	5	5	2	2	6	2	5	4	4	4	4	4	4	3	2	5	6
25	5	4	4	6	6	3	3	5	4	3	5	3	5	5	5	5	4	3	3	6	6	6	6	6	4	6	4	6	5	3	5	6
26	4	3	3	5	5	4	5	5	5	4	6	6	6	6	4	6	5	3	3	5	5	5	5	6	4	6	6	6	6	5	4	5
27	6	5	6	6	6	5	4	6	6	5	3	4	4	4	6	5	6	5	5	6	6	5	4	6	4	6	6	6	4	4	5	4
28	5	5	4	6	6	5	6	6	5	5	6	4	5	4	5	6	6	2	4	6	5	6	5	5	5	4	4	4	4	5	5	4
29	5	4	5	5	6	6	6	5	5	5	4	4	6	4	5	5	6	6	5	6	6	6	6	6	5	6	5	5	5	6	5	5
30	6	5	4	6	6	6	5	6	5	4	6	5	6	5	6	5	5	4	4	6	6	6	5	6	5	5	6	6	6	4	5	5
31	5	5	6	6	6	4	5	6	4	4	6	5	5	6	6	6	6	4	4	6	6	5	5	6	4	6	6	6	6	4	5	5
32	5	4	5	6	6	4	4	6	5	5	5	4	4	6	6	6	5	5	5	6	6	6	6	5	6	5	5	5	6	6	4	5
33	6	5	5	5	6	3	4	5	5	6	4	3	3	5	3	2	2	3	2	5	5	6	5	6	5	6	5	6	3	3	4	5
34	6	6	6	5	6	5	6	4	4	4	4	3	4	5	5	5	5	4	4	5	6	6	6	4	6	5	5	4	5	4	5	5
35	5	5	4	4	5	3	4	6	6	6	3	4	5	6	4	4	3	4	4	6	5	6	6	5	4	4	6	6	6	6	5	4
36	6	6	6	6	6	4	6	6	4	5	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5
37	5	4	4	4	5	5	6	6	6	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
38	6	4	4	6	6	5	5	5	5	5	2	3	3	4	5	5	5	5	3	6	6	6	6	6	6	6	5	5	5	6	5	5
39	4	2	3	4	5	4	5	5	4	4	5	5	4	6	3	3	3	4	4	4	5	5	5	4	5	3	4	5	5	5	6	5
40	5	5	4	4	5	4	3	4	6	3	2	3	4	4	3	4	5	5	2	5	6	6	5	3	5	5	4	3	5	4	2	3

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
41	6	5	5	5	6	3	6	4	4	4	3	3	4	4	5	3	4	4	4	4	4	4	4	4	4	4	6	5	4	5	5	5
42	6	5	4	5	5	5	6	6	6	6	4	4	5	3	6	6	6	5	5	6	6	6	6	6	6	6	6	6	6	6	5	5
43	6	3	4	6	5	3	5	5	4	4	5	6	5	6	4	5	4	6	6	6	6	6	5	4	5	5	6	6	4	3	6	3
44	5	5	5	4	6	5	5	5	5	5	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	6	6	6	6	6	5
45	3	2	3	4	6	6	3	3	4	6	4	5	4	5	4	5	4	3	3	5	5	5	5	5	5	4	4	5	5	5	4	3
46	4	4	3	3	4	4	4	5	5	4	5	4	3	5	5	4	5	3	5	4	5	4	4	5	5	4	5	4	5	5	4	4
47	4	4	3	4	4	4	5	6	5	6	4	4	4	4	3	3	3	4	3	4	4	4	4	4	4	4	4	4	5	6	6	6
48	5	6	5	5	6	4	6	6	5	5	5	3	4	5	4	4	4	4	3	6	5	5	5	6	6	6	6	6	6	5	5	5
49	5	5	5	3	6	6	6	5	6	6	5	3	4	6	5	5	5	3	5	5	5	6	6	6	6	6	5	5	6	6	6	6
50	5	4	4	5	5	4	5	5	4	4	2	2	2	3	5	5	5	4	4	6	6	6	6	6	6	6	5	5	5	5	4	4
51	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	1	1	6	6	6	6	6	6	6	6	6	6	6	6	1
52	5	4	4	6	5	4	5	5	5	5	3	2	1	4	5	5	5	4	5	3	5	5	4	4	4	3	4	4	5	5	3	4
53	5	5	5	5	5	5	5	5	4	5	3	4	4	5	4	4	4	5	5	5	5	5	5	4	6	4	5	5	5	5	5	4
54	5	5	5	5	6	4	5	5	4	4	3	3	3	4	4	4	4	3	3	5	5	6	5	4	5	4	5	5	5	4	6	3
55	5	6	4	4	4	5	5	5	4	5	2	1	1	2	5	5	5	4	3	4	4	5	5	5	4	4	5	4	4	5	5	5
56	5	5	5	5	5	5	5	5	5	6	1	1	1	2	2	2	1	2	2	2	6	5	5	5	5	5	5	5	5	5	5	2
57	6	6	6	6	6	6	6	6	6	3	1	1	1	1	4	4	4	6	6	4	6	4	4	4	4	4	6	6	6	6	6	6
58	5	5	5	6	6	6	6	5	6	6	2	2	2	2	6	6	6	5	5	5	5	6	5	5	6	3	4	4	4	5	3	3
59	6	5	5	6	6	6	6	6	6	6	1	2	2	4	3	3	6	5	5	6	5	6	6	5	4	4	6	6	6	6	5	5
60	4	5	4	4	4	4	4	4	5	4	3	5	4	4	5	5	4	3	3	5	5	4	3	4	4	4	4	4	4	4	3	3
61	4	3	4	3	5	5	5	5	3	4	3	3	3	4	3	4	4	4	4	5	4	6	5	5	5	5	5	5	4	5	5	5
62	2	3	3	3	3	3	3	3	3	4	4	4	3	4	4	4	4	3	3	5	5	5	5	5	5	5	6	6	6	6	6	6

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
63	6	6	5	6	6	2	5	5	3	3	4	4	4	5	2	3	3	5	4	3	4	5	4	3	5	2	6	6	5	5	5	3
64	1	1	1	1	1	1	1	1	1	1	2	2	2	4	3	3	4	3	4	6	6	6	5	4	6	5	3	3	6	6	6	3
65	5	5	5	5	5	4	4	5	4	5	2	2	2	5	5	3	2	2	2	5	5	5	5	5	5	4	4	4	5	5	5	2
66	6	6	3	6	6	3	6	6	6	6	1	1	1	3	6	6	6	1	1	6	6	6	6	6	6	6	6	6	6	6	6	6
67	6	6	6	6	6	6	6	6	6	5	4	4	4	4	4	5	5	5	5	6	6	6	4	5	6	3	6	5	5	6	4	5
68	4	4	3	1	1	4	4	5	5	4	2	2	2	2	4	4	4	4	4	5	5	5	5	5	5	4	3	3	5	5	4	5
69	4	3	4	3	3	4	3	4	4	3	2	2	4	2	3	3	4	6	5	2	6	6	3	3	4	1	3	4	4	4	3	2
70	5	4	5	5	5	5	5	5	5	5	2	3	2	2	2	2	2	3	3	2	2	3	4	3	2	4	4	2	5	3	3	4
71	5	4	4	6	6	4	6	6	6	6	2	3	2	3	5	5	5	5	3	6	4	6	6	5	5	5	4	5	5	5	3	3
72	4	4	4	4	4	4	4	4	4	4	2	2	2	2	2	3	3	4	4	5	5	5	6	5	5	5	4	4	4	3	3	4
73	6	6	3	6	6	5	6	6	5	5	4	4	4	5	5	5	5	4	4	6	5	6	6	5	6	5	6	6	6	5	6	6
74	5	4	3	4	4	4	4	4	4	4	3	2	3	2	4	4	4	3	3	4	4	4	5	5	5	5	5	4	4	4	4	3
75	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5	4	4	5	5	5	2	5	5	4	5	4	4	4	3	5	3	4
76	5	5	5	5	6	6	6	6	6	6	1	2	2	3	4	4	4	4	4	5	6	6	5	5	5	5	6	6	6	6	5	5
77	5	5	5	5	5	5	5	5	5	5	2	2	2	2	4	4	4	3	2	4	4	5	4	3	5	3	4	4	4	4	4	3
78	6	6	6	6	5	6	6	6	6	6	2	2	5	5	5	5	5	2	2	6	6	6	6	6	6	5	6	5	6	6	6	2
79	6	5	5	4	4	4	4	4	4	6	3	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5
80	6	6	6	6	6	6	6	6	6	5	5	3	5	4	4	5	4	5	4	6	3	6	6	6	6	6	5	6	5	5	6	5
81	4	4	4	6	6	4	6	6	6	4	5	6	6	6	5	5	5	2	2	6	6	6	6	6	5	5	6	6	5	6	6	6
82	5	5	5	5	6	4	5	5	5	5	2	2	2	2	3	3	3	4	4	6	5	5	5	5	5	5	5	5	5	5	5	5
83	3	2	4	4	5	4	4	5	4	5	2	2	2	4	5	5	5	4	3	5	5	4	5	5	4	4	4	4	4	5	5	5
84	5	5	5	5	5	5	6	6	6	6	5	4	4	4	5	5	5	5	5	5	4	6	5	4	6	5	5	5	4	5	5	5

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
85	6	4	3	6	6	5	5	6	5	4	4	5	4	5	6	3	3	6	4	5	3	5	5	5	3	5	3	5	5	5	6	6
86	6	5	5	5	5	2	5	6	6	5	5	5	5	6	5	5	5	2	2	6	6	6	6	6	5	5	6	6	5	5	5	6
87	6	6	6	6	6	5	6	6	6	6	2	2	2	2	2	2	2	4	4	5	5	5	5	4	6	5	4	4	5	5	5	6
88	6	6	5	6	5	4	5	6	4	5	2	2	2	3	5	5	5	6	4	5	6	6	5	5	6	5	4	4	6	5	4	4
89	2	2	2	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
90	5	5	5	6	6	6	6	6	6	2	1	1	1	1	3	3	3	5	5	6	6	6	6	6	6	6	6	5	5	5	5	5
91	5	5	5	5	5	5	5	5	5	5	5	2	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
92	2	1	2	2	2	5	5	5	5	3	5	5	6	6	5	5	5	3	3	4	5	5	5	5	5	5	6	6	6	6	6	6
93	6	5	5	5	6	5	5	6	5	3	1	3	2	6	2	2	3	5	2	6	5	6	5	5	6	5	6	6	6	5	4	3
94	5	4	4	5	5	5	5	5	5	5	4	3	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	3	3	3
95	1	6	5	6	6	3	6	6	4	6	5	3	4	5	5	4	5	2	1	5	6	6	4	5	6	6	6	6	6	6	6	6
96	5	5	5	5	5	5	5	5	5	5	3	3	3	3	4	4	4	5	4	5	5	6	5	5	5	5	6	6	6	5	5	4
97	6	6	6	6	6	6	6	6	6	4	2	2	2	4	2	2	2	5	5	5	6	6	6	4	5	4	6	6	6	6	4	4
98	5	5	5	5	5	6	6	6	6	5	3	3	3	2	2	2	2	4	3	5	6	6	5	5	6	4	5	5	6	6	5	5
99	6	6	6	6	6	6	6	6	1	1	2	2	2	2	2	6	6	1	1	6	6	6	6	6	6	1	3	3	6	3	4	4
100	6	6	5	6	6	6	6	6	6	6	6	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5
101	5	4	4	4	4	4	4	5	5	4	4	4	4	5	3	3	3	5	5	4	4	4	5	3	5	3	4	5	5	5	6	3
102	6	5	6	6	6	6	6	6	6	6	6	5	5	5	4	4	4	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6
103	6	6	6	6	6	6	6	6	6	6	2	1	1	3	4	4	4	4	4	6	6	6	6	6	6	6	6	6	6	6	4	4
104	6	4	4	5	6	5	6	6	6	6	4	5	5	5	2	2	2	5	5	6	6	6	6	4	6	4	5	5	5	6	4	2
105	6	6	3	5	4	4	5	5	4	5	4	4	4	4	5	5	4	5	4	5	5	6	5	5	4	4	6	6	5	6	6	5
106	5	5	5	5	6	6	6	6	6	6	4	4	4	4	3	3	3	4	4	4	6	6	6	6	6	4	4	6	4	6	6	4

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
107	6	6	6	6	6	6	6	5	5	3	2	2	6	5	3	1	5	2	1	6	6	6	6	3	1	1	1	1	1	1	2	1
108	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	5	4	5	3	5	4	5	4
109	6	5	6	5	6	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	6	5	5	5	5	5	5	6	5	5	5	5
110	6	2	3	6	6	6	6	6	6	4	4	5	5	6	4	4	4	4	3	5	5	5	6	5	6	5	6	6	6	5	4	4
111	6	6	6	6	6	6	6	6	6	6	6	5	4	5	6	6	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6
112	5	4	4	5	4	3	5	5	5	4	4	3	4	5	3	4	4	4	4	4	4	5	5	4	5	4	5	5	4	3	3	3
113	6	5	6	6	6	6	6	6	6	6	2	2	2	2	4	4	4	5	5	6	6	6	5	5	5	5	5	5	5	5	5	5
114	5	6	5	5	5	5	5	5	6	6	6	3	2	5	5	6	5	5	3	5	5	5	6	5	5	5	5	6	6	5	6	5
115	4	4	4	5	4	5	5	5	5	5	3	3	3	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4
116	6	5	5	6	6	6	6	6	6	6	2	3	3	4	5	5	5	5	5	6	6	6	5	5	4	4	6	4	6	6	5	5
117	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4
118	6	6	3	6	6	6	6	6	6	6	1	5	6	6	6	6	6	6	3	6	6	6	6	6	6	6	6	6	6	6	6	6
119	6	4	4	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
120	4	4	4	6	6	4	5	5	5	3	6	6	6	6	4	4	5	1	1	6	6	6	6	6	5	5	6	6	6	6	6	6
121	6	6	6	6	6	4	6	6	6	5	2	4	5	5	6	6	6	4	4	5	5	5	6	5	5	5	5	5	5	6	6	6
122	6	6	6	6	6	6	6	6	6	6	5	5	6	6	6	6	6	6	6	6	6	5	4	5	5	5	6	6	6	6	5	5
123	5	5	5	6	5	5	5	5	5	4	3	2	2	2	3	4	3	4	2	4	4	4	6	5	4	5	3	3	3	3	4	4
124	6	6	6	6	6	5	6	6	6	6	5	1	1	1	2	1	1	4	5	5	5	5	6	5	5	6	4	4	5	4	3	2
125	6	6	6	6	6	6	6	6	6	6	1	1	1	1	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
126	6	2	3	5	5	5	5	5	3	3	2	2	2	3	4	5	3	3	3	5	5	5	5	4	5	4	4	5	4	4	4	4
127	6	6	6	6	6	6	6	6	6	6	1	1	2	2	3	3	3	5	5	6	6	6	6	6	6	6	4	4	5	4	6	5
128	6	6	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	5

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
129	5	5	2	2	2	2	5	5	2	5	5	2	5	5	3	3	3	3	3	5	5	5	5	5	5	5	5	5	5	5	5	5
130	5	4	5	4	5	5	5	5	5	6	2	2	3	3	3	3	3	4	4	3	4	4	5	3	4	4	4	4	4	4	5	4
131	5	4	5	5	5	4	5	6	5	5	4	4	4	4	4	4	5	4	4	5	5	6	5	4	5	4	5	4	5	5	4	3
132	6	5	6	5	5	5	5	6	6	5	3	3	4	4	3	4	4	4	6	5	5	6	5	5	5	5	5	5	5	3	4	5
133	6	5	5	5	5	5	5	5	5	3	3	2	5	5	5	5	5	3	3	5	5	5	4	5	5	5	5	5	5	4	5	5
134	6	5	4	5	5	4	4	5	5	4	5	4	5	5	6	6	6	1	1	5	5	5	5	5	5	5	5	5	5	5	5	6
135	3	4	3	3	5	3	3	4	4	4	3	3	3	4	4	4	4	3	3	3	3	4	4	4	4	4	4	4	4	5	5	4
136	5	3	4	4	2	4	5	5	5	4	5	5	5	5	2	2	2	4	4	3	4	5	5	4	5	3	5	5	5	5	2	2
137	5	5	5	5	5	5	5	5	5	5	3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
138	6	5	5	5	5	5	5	5	5	5	2	2	2	3	4	5	5	4	4	6	6	5	5	4	4	3	3	4	5	3	5	5
139	3	4	5	5	6	5	6	6	6	6	6	6	6	6	6	5	6	4	2	6	2	4	4	6	4	4	6	6	6	5	6	6
140	5	5	6	6	6	6	6	5	5	5	6	5	5	5	5	6	6	6	5	5	6	6	6	6	6	6	5	6	5	5	5	5
141	5	5	5	5	5	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	6	4	5	4	4	4	5	3	4	3
142	5	5	5	5	5	4	5	4	4	5	2	2	2	2	4	4	4	3	3	5	5	5	5	5	5	4	4	4	5	4	4	4
143	4	3	4	4	4	4	6	6	6	6	2	1	1	2	6	5	5	6	6	5	5	6	6	4	6	4	3	4	5	4	2	2
144	1	1	1	4	4	4	4	5	5	6	3	3	3	3	4	4	4	6	5	4	5	6	5	5	6	4	6	6	6	6	6	6
145	5	6	4	6	6	6	5	5	4	4	5	5	4	6	5	6	5	5	4	5	5	6	6	5	6	5	6	6	5	6	5	5
146	5	5	4	6	6	4	4	5	4	6	2	2	3	4	5	5	4	4	4	6	5	6	5	5	5	5	5	5	5	5	5	5
147	2	2	4	2	3	4	2	2	3	2	1	5	5	6	3	3	3	6	3	3	1	1	6	6	6	4	6	6	3	3	6	3
148	5	5	5	5	6	5	5	6	5	5	2	4	5	5	5	5	5	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5
149	6	5	4	4	4	5	5	4	5	5	5	4	6	5	6	6	5	6	6	5	6	6	5	4	4	5	4	6	6	5	5	4
150	4	4	4	4	4	4	4	4	4	4	2	1	3	6	4	4	4	4	3	6	6	6	4	4	4	4	4	4	4	4	4	4

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
151	6	5	5	5	5	5	5	5	5	3	4	2	2	4	5	5	5	4	3	5	5	5	5	5	5	4	4	5	5	4	3	3
152	2	2	3	4	4	3	4	4	5	5	6	6	6	6	4	4	5	3	3	4	3	4	4	5	4	4	6	6	4	6	6	6
153	6	6	2	6	5	2	6	4	2	5	3	3	5	5	5	5	5	5	2	4	6	6	4	4	5	5	6	6	6	5	5	6
154	6	6	6	6	6	6	6	6	6	6	1	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
155	6	6	6	6	6	5	6	6	5	6	2	1	4	4	4	5	6	5	5	5	6	6	6	4	5	4	5	5	5	6	6	4
156	5	4	5	5	5	5	6	6	5	5	2	2	2	2	4	4	4	5	5	5	5	5	5	4	5	4	4	4	4	4	4	4
157	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	5	4	4
158	6	6	6	6	6	6	6	6	6	6	4	4	4	4	4	6	6	6	6	6	1	6	6	6	6	6	6	6	6	6	6	6
159	6	6	5	6	6	4	4	6	6	6	5	6	5	5	5	6	4	5	6	3	6	6	5	6	6	5	6	6	5	6	4	5
160	6	6	6	6	6	6	6	6	6	6	3	6	6	6	6	6	6	5	6	6	6	4	6	6	6	6	6	6	5	4	6	6
161	2	3	3	3	5	3	5	5	5	6	5	5	5	5	6	5	5	1	1	6	6	6	6	6	6	6	5	5	6	6	6	5
162	5	6	5	6	5	5	5	4	6	5	3	3	2	2	2	2	2	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5
163	3	4	4	5	5	3	5	4	4	4	3	3	2	3	3	4	5	2	3	5	6	6	6	5	6	6	4	4	3	2	2	3
164	4	4	4	4	4	5	5	5	5	5	3	2	2	3	4	5	4	4	4	6	6	5	5	4	6	4	6	6	6	6	6	6
165	5	4	1	5	6	3	6	6	3	6	5	4	3	6	5	5	5	1	1	6	6	6	6	5	6	5	6	6	6	6	5	3
166	6	5	6	6	6	6	6	6	6	6	6	5	5	6	3	4	5	3	3	5	6	6	6	6	6	6	6	6	6	6	6	6
167	5	4	4	4	4	2	4	4	5	4	2	1	1	2	1	1	2	4	2	3	4	5	5	5	5	4	2	2	2	4	2	1
168	6	6	4	6	6	3	5	5	5	5	2	2	5	5	6	5	5	2	2	6	5	5	6	6	6	6	4	5	6	6	6	4
169	5	4	5	6	5	6	5	4	6	3	3	4	5	5	4	4	4	3	3	5	4	4	5	4	5	4	6	6	6	5	6	6
170	5	4	2	4	4	5	5	5	5	5	4	5	5	5	5	5	5	4	4	5	4	4	5	5	5	5	5	5	5	5	5	5
171	5	5	4	4	4	3	5	5	6	6	3	4	5	6	4	4	3	4	4	6	5	6	6	5	4	4	6	6	6	6	5	4
172	2	2	3	4	4	3	4	4	5	5	6	6	6	6	4	4	5	3	3	4	3	4	4	5	4	4	6	6	4	6	6	6

NO	PKR			PKP			PA				ED				EP			SG		AP			MP				PP					
	1	2	3	1	2	3	1	2	3	4	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	5	6
173	4	4	4	6	6	4	5	5	5	3	6	6	6	6	4	4	5	1	1	6	6	6	6	6	5	5	6	6	6	6	6	6
174	4	4	3	3	4	4	4	5	5	4	5	4	3	5	5	4	5	3	5	4	5	4	4	5	5	4	5	4	5	5	4	4
175	4	4	3	5	4	4	5	5	4	6	3	3	3	4	4	4	5	3	3	4	5	5	4	4	4	3	3	4	5	5	3	3
176	4	4	3	4	4	5	4	4	4	4	4	5	5	4	4	5	6	4	4	5	5	5	5	5	5	5	4	5	5	5	5	5
177	5	4	4	5	4	3	5	6	5	2	4	4	4	5	4	4	4	4	4	5	6	6	5	4	6	4	5	5	5	4	3	3
178	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
179	6	6	5	5	6	6	6	6	6	2	2	2	2	5	6	6	6	2	2	2	5	5	5	5	5	5	5	6	6	6	6	6
180	4	3	4	4	4	4	5	5	5	4	5	5	3	6	4	4	4	4	4	3	3	5	4	4	4	4	6	6	3	4	4	4

Klasifikasi Responden Berdasarkan Jenis Kelamin

	Jumlah	Persentase
Laki-laki	94	52%
Perempuan	86	48%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Kelompok Usia

Rentang Usia	Jumlah	Persentase
< 20 tahun	0	0%
20-29 tahun	87	48%
30-39 tahun	52	29%
40-49 tahun	27	15%
50-59 tahun	14	8%
> 59 tahun	0	0%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Sektor Industri Pekerjaan

Rentang Usia	Jumlah	Persentase
< 20 tahun	0	0%
20-29 tahun	87	48%
30-39 tahun	52	29%
40-49 tahun	27	15%
50-59 tahun	14	8%
> 59 tahun	0	0%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Kategori Sektor Industri Keuangan

Kategori Sektor Industri	Jumlah	Persentase
Perbankan	87	48%
Asuransi	25	14%
Perusahaan Sekuritas	14	8%
Lembaga Pembiayaan (Leasing, Anjak Piutang, dsb.)	22	12%
Koperasi Simpan Pinjam	3	2%
Pegadaian	2	1%
Lainnya	27	15%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Wilayah Bekerja

Provinsi	Jumlah	Persentase
DKI Jakarta	76	42%
Daerah Istimewa Yogyakarta	56	31%

Provinsi	Jumlah	Persentase
Jawa Tengah	15	8%
Jawa Barat	13	7%
Jawa Timur	9	5%
Banten	3	2%
Sumatera Selatan	2	1%
Lampung	2	1%
Bali	1	1%
Gorontalo	1	1%
Kepulauan Riau	1	1%
Kalimantan Timur	1	1%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Lama Bekerja

Rentang Tahun	Jumlah	Persentase
1-3 tahun	51	28%
4-7 tahun	44	24%
7-10 tahun	24	13%
>10 tahun	61	34%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Bidang Profesi

Bidang profesi	Jumlah	Persentase
Akuntansi & Keuangan	63	35%
Administrasi	16	9%
General Affair	2	1%
HRD	11	6%
Pemasaran & Penjualan	18	10%
Teknologi Informasi	10	6%
Lainnya	60	33%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Penggunaan Perangkat Elektronik Dalam Bekerja

	Jumlah	Persentase
Ya	180	100%
Tidak	0	0%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Pengalaman Menjadi Korban Kejahatan Siber Keuangan

	Jumlah	**Persentase**
Pernah	68	38%
Tidak Pernah	112	62%
Total	**180**	**100%**

Klasifikasi Responden Berdasarkan Pengalaman Terkait Serangan Kejahatan Siber Keuangan

No	Bentuk Kejahatan Siber yang Pernah Dialami
1	Kejahatan Carding, Pemerasan Siber, Penipuan Link Palsu
2	Penipuan Link Palsu, Penipuan Pesan Berisi APK
3	Kejahatan Carding
4	Penipuan Link Palsu, Penipuan Pesan Berisi APK
5	Pemerasan Siber, Penipuan Link Palsu, Penipuan Pesan Berisi APK
6	Penipuan OTP
7	Penipuan Link Palsu, Penipuan Pesan Berisi APK
8	Pemerasan Siber, Penipuan Link Palsu, Penipuan Pesan Berisi APK
9	Lainnya
10	Penipuan Link Palsu, Penipuan Pesan Berisi APK
11	Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
12	Lainnya
13	Kejahatan Carding
14	Penipuan Link Palsu
15	Penipuan OTP
16	Serangan Adware
17	Lainnya
18	Pemerasan Siber, Penipuan OTP, Penipuan Link Palsu
19	Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
20	Penipuan Pesan Berisi APK
21	Lainnya
22	Penipuan Link Palsu
23	Penipuan OTP

No	Bentuk Kejahatan Siber yang Pernah Dialami
24	Serangan Adware, Penipuan Link Palsu
25	Penipuan OTP, Penipuan Link Palsu
26	Penipuan Link Palsu
27	Pemerasan Siber
28	Kejahatan Carding, Penipuan Link Palsu, Penipuan Pesan Berisi APK
29	Serangan Adware, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
30	Penipuan Link Palsu
31	Penipuan OTP, Penipuan Pesan Berisi APK
32	Penipuan Link Palsu
33	Penipuan Pesan Berisi APK
34	Serangan Adware, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
35	Penipuan Link Palsu, Penipuan Pesan Berisi APK
36	Penipuan OTP
37	Lainnya
38	Serangan Adware, Penipuan Link Palsu, Penipuan Pesan Berisi APK
39	Penipuan Link Palsu
40	Lainnya
41	Kejahatan Carding, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
42	Penipuan OTP
43	Kejahatan Carding
44	Penipuan Pesan Berisi APK
45	Penipuan Link Palsu, Lainnya
46	Penipuan Pesan Berisi APK, Lainnya
47	Lainnya

No	Bentuk Kejahatan Siber yang Pernah Dialami
48	Serangan Adware
49	Kejahatan Carding, Serangan Adware, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
50	Serangan Adware
51	Penipuan OTP, Penipuan Link Palsu
52	Penipuan Link Palsu
53	Lainnya
54	Penipuan OTP, Penipuan Link Palsu
55	Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
56	Serangan Adware, Penipuan Pesan Berisi APK
57	Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
58	Lainnya
59	Kejahatan Carding, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
60	Serangan Adware, Penipuan Link Palsu, Lainnya
61	Serangan Adware, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
62	Lainnya
63	Penipuan Link Palsu
64	Serangan Adware
65	Penipuan Pesan Berisi APK
66	Penipuan Pesan Berisi APK
67	Kejahatan Carding
68	Penipuan OTP
69	Penipuan OTP
70	Lainnya
71	Penipuan Link Palsu

No	Bentuk Kejahatan Siber yang Pernah Dialami
72	Penipuan Pesan Berisi APK, Lainnya
73	Penipuan Link Palsu
74	Serangan Adware, Penipuan Link Palsu, Penipuan Pesan Berisi APK
75	Serangan Adware, Penipuan Link Palsu
76	Penipuan OTP, Penipuan Link Palsu
77	Penipuan Link Palsu
78	Serangan Adware, Penipuan Link Palsu, Penipuan Pesan Berisi APK
79	Pemerasan Siber, Penipuan Link Palsu, Penipuan Pesan Berisi APK
80	Penipuan Link Palsu
81	Penipuan Link Palsu
82	Penipuan Link Palsu, Penipuan Pesan Berisi APK
83	Serangan Adware, Penipuan OTP, Penipuan Link Palsu, Penipuan Pesan Berisi APK
84	Penipuan Link Palsu
85	Penipuan Link Palsu
86	Penipuan Link Palsu
87	Penipuan OTP, Penipuan Pesan Berisi APK
88	Penipuan Pesan Berisi APK
89	Penipuan Link Palsu
90	Penipuan Pesan Berisi APK
91	Penipuan Pesan Berisi APK
92	Lainnya
93	Kejahatan Carding
94	Serangan Adware
95	Pemerasan Siber

No	Bentuk Kejahatan Siber yang Pernah Dialami
96	Serangan Adware, Penipuan Link Palsu, Penipuan Pesan Berisi APK
97	Penipuan OTP
98	Serangan Adware, Penipuan Link Palsu
99	Penipuan Pesan Berisi APK
100	Penipuan Pesan Berisi APK
101	Penipuan Link Palsu, Penipuan Pesan Berisi APK
102	Penipuan Link Palsu

Lampiran 3.

Hasil Analisis Data

Uji Validitas Konvergen

Variabel	Kode	Loading	AVE	Keterangan
Persepsi Kerentanan	PKR1	0.872	0.760	Valid
	PKR2	0.894		
	PKR3	0.849		
Persepsi Keparahan	PKP1	0.889	0.713	Valid
	PKP2	0.897		
	PKP3	0.737		
Persepsi Ancaman	PA1	0.877	0.654	Valid
	PA2	0.899		
	PA3	0.772		
	PA4	0.664		
Efikasi Diri	ED1	0.817	0.775	Valid
	ED2	0.916		
	ED3	0.909		
	ED4	0.875		
Efektivitas Perlindungan	EP1	0.912	0.858	Valid
	EP2	0.957		
	EP3	0.910		
Safeguard Cost	SC1	0.906	0.879	Valid
	SC2	0.968		
Antisipasi Penyesalan	AP1	0.816	0.685	Valid
	AP2	0.798		
	AP3	0.868		
Motivasi Penghindaran Kejahatan Siber Keuangan	MP 1	0.775	0.655	Valid
	MP2	0.863		
	MP3	0.759		
	MP4	0.853		
Perilaku Penghindaran Kejahatan Siber Keuangan	PP1	0.837	0.618	Valid
	PP2	0.859		
	PP3	0.772		
	PP4	0.760		
	PP5	0.790		
	PP6	0.685		

Uji Validitas Diskriminan

	AP	EP	ED	MP	PP	PA	PKP	PKR	SC	PKP X PKR
AP										
EP	0.395									
ED	0.093	0.285								
MP	0.707	0.381	0.162							
PP	0.418	0.460	0.390	0.621						
PA	0.506	0.309	0.060	0.528	0.480					
PKP	0.540	0.352	0.067	0.506	0.397	0.862				
PKR	0.430	0.166	0.125	0.362	0.189	0.708	0.864			
SC	0.123	0.121	0.069	0.135	0.177	0.331	0.252	0.303		
PKP X PKR	0.112	0.110	0.029	0.090	0.116	0.454	0.521	0.477	0.040	

Uji Reliabilitas

Variabel	*Composite Reliability*	*Cronbach's Alpha*
Persepsi Kerentanan (PKR)	0.905	0.842
Persepsi Keraparahan (PKP)	0.881	0.794
Persepsi Ancaman (PA)	0.882	0.823
Efikasi Diri (ED)	0.932	0.902
Efektivitas Perlindungan (EP)	0.948	0.918
Safeguard Cost (SC)	0.936	0.871
Antisipasi Penyesalan (AP)	0.867	0.772
Motivasi Penghindaran Kejahatan Siber Keuangan (MP)	0.883	0.824
Perilaku Penghindaran Kejahatan Siber Keuangan (PP)	0.906	0.876

Uji *R-Square*

Variabel	*R-Square*	*R-Square Adjusted*
Persepsi Ancaman	0.545	0.537
Motivasi Penghindaran Kejahatan Siber Keuangan	0.391	0.374
Perilaku Penghindaran Kejahatan Siber Keuangan	0.294	0.290

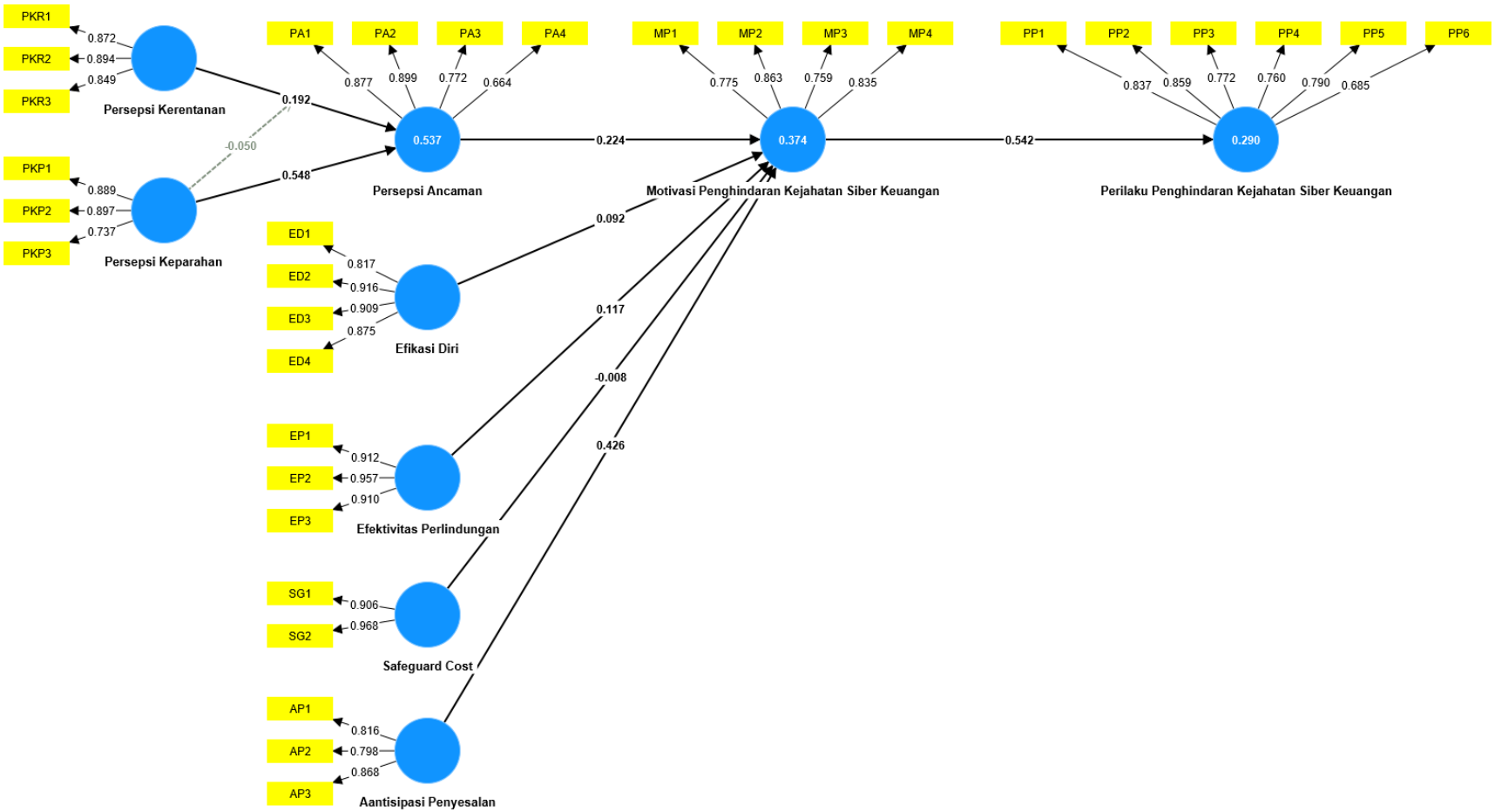
Nilai AVE dan *R-Square*

Variabel	AVE	R-Square
Antisipasi Penyesalan	0,685	0,545
Motivasi Penghindaran Kejahatan Siber Keuangan	0,655	0,391
Perilaku Penghindaran Kejahatan Siber Keuangan	0,618	0,294

Uji *Path Coefficient* dan *Statistical Significance*

	Nilai Koefisien (Beta)	Standar Deviasi (STDEV)	*T Statistics*	*P Values*
PKR → PA	0.192	0.093	2.079	0.038
PKP → PA	0.548	0.085	6.476	0.000
PKR x PKP → PA	-0.050	0.074	**0.671**	**0.503**
PA → MP	0.224	0.077	2.930	0.003
ED → MP	0.092	0.063	1.461	**0.144**
EP → MP	0.117	0.069	1.685	**0.092**
SC → MP	-0.008	0.070	**0.115**	**0.908**
AP → MP	0.426	0.093	4.563	0.000
MP → PP	0.542	0.064	8.524	0.000

LAMPIRAN 4


PKR1
PKR2
PKR3
0.872
0.894
0.849
Persepsi Kerentanan
PKP1
PKP2
PKP3
0.889
0.897
0.737
Persepsi Keparahan
0.192
-0.050
0.548
PA1
PA2
PA3
PA4
0.877
0.899
0.772
0.664
0.537
Persepsi Ancaman
0.224
MP1
MP2
MP3
MP4
0.775
0.863
0.759
0.835
0.374
Motivasi Penghindaran Kejahatan Siber Keuangan
0.542
PP1
PP2
PP3
PP4
PP5
PP6
0.837
0.859
0.772
0.760
0.790
0.685
0.290
Perilaku Penghindaran Kejahatan Siber Keuangan
ED1
ED2
ED3
ED4
0.817
0.916
0.909
0.875
Efikasi Diri
0.092
EP1
EP2
EP3
0.912
0.957
0.910
Efektivitas Perlindungan
0.117
SG1
SG2
0.906
0.968
Safeguard Cost
-0.008
AP1
AP2
AP3
0.816
0.798
0.868
Aantisipasi Penyesalan
0.426