BAB I

PENDAHULUAN

1.1 Latar Belakang

Hadirnya transaksi elektronik, diharapkan dapat membantu masyarakat agar semakin efisien dalam melakukan kegiatan ekonomi. Untuk proses transaksi yang aman dan efektif, dibutuhkan pemahaman dari masyarakat sebagai pengguna. Penggunaan transaksi elektronik tidak dapat terhindar dari risiko yang mungkin saja terjadi karena tindakan kejahatan seringkali dihubungkan dengan transaksi keuangan. Industri keuangan sering dijadikan sebagai incaran penipuan karena targetnya yaitu mendapatkan uang. Didukung dengan sistem teknologi dan informasi yang mempermudah pelaku kejahatan menemukan celah untuk memperoleh sebuah data yang berujung dapat mengakses dana milik seseorang.

Penipuan dalam transaksi elektronik sering dilakukan dengan modus *social engineering* atau rekayasa sosial.[1] Menurut Karren J Banne, penipuan ini dimulai dengan tindakan manipulatif atau berpura-pura sebagai seseorang yang berasal dari suatu organisasi atau lembaga dengan modus memberikan informasi kepada pengguna.[2] Modus tersebut digunakan untuk memanfaatkan kelengahan manusia yang seringkali lalai atau mudah percaya.[3] Sistem yang sudah dilindungi dengan

[1] Pusat Penelitian Sekretariat Jenderal dan Badan Keahlian Dewan Perwakilan Rakyat Republik Indonesia, "Tindak Pidana Penipuan Transaksi Elektronik Upaya Pencegahan oleh Perbankan", <https://berkas.dpr.go.id/puslit/files/hasil_diskusi/hasil-diskusi-42.doc>, diakses 7 Agustus 2022.
[2] Onny Rafizan, "Analisis Penyerangan *Social Engineering*". Karya Ilmiah, Magelang: Balitbang SDM Kominfo, 2011, hal. 120.
[3] Dani Indra Junaedi, "Antisipasi Dampak *Social Engineering* Pada Bisnis Perbankan", Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK, Vol 11, Nomor 1, Mei 2017, hal. 3.

perangkat lunak atau keras secanggih apa pun tidak akan terlepas dari adanya kelemahan yang bertitik tumpu pada manusia itu sendiri sebagai pengguna.[4] Modus *social engineering* ini sudah terjadi sejak dahulu, namun modus ini kembali hangat pada era digital di mana perbankan mulai menggunakan transaksi elektronik.[5] Nasabah selaku pengguna juga memiliki kepentingan terkait keamanan sebuah sistem. Richardus Eko Indrajit memberikan sebuah pernyataan bahwa dalam jaringan keamanan, manusia menjadi bagian yang dianggap paling lemah.[6] Dalam penipuan rekayasa sosial, terdapat salah satu metode yang memposisikan manusia sebagai celah untuk melakukan kejahatan yaitu *phising*. Serangan *phising* berkembang di dunia maya dengan sangat cepat.[7]

Phising adalah tindakan mencuri informasi seseorang yang digunakan untuk mengakses sebuah akun dengan cara memberi informasi dan muatan palsu.[8] Secara umum, *phising* diawali dengan pesan yang menggunakan gaya bahasa yang sopan dan baik. Gaya bahasa yang digunakan inilah menjadi cara di mana dalam mengelabui seseorang di mana seolah-olah pesan yang diterima berasal dari lembaga resmi.[9] Pencurian ini telah diatur dalam Pasal 35 Undang-Undang Nomor

---

[4] Hendri Ahmadian dan Aulia Sabri, "Teknik Penyerangan *Phishing* Pada *Social Engineering* Menggunakan Set Dan Pencegahannya", Djtechno: Journal of Information Technology Research Vol. 2, Nomor 1, Juli 2021, hal. 15.

[5] Jasa Keuangan, "*OJK BiSa eps #1: Kupas Soceng "Social Engineering"*", <https://www.youtube.com/watch?v=OxLz0noVLaA>, diakses 13 September 2022.

[6] Richardus Eko Indrajit, "Seluk Beluk Teknik Social Engineering", <https://adoc.pub/seluk-beluk-teknik-social-engineering.html>, diakses 27 Agustus 2022.

[7] Agil Nofiyan dan Mushlihudin, "Analisis Forensik pada *Web Phishing* Menggunakan Metode *National Institute Of Standards And Technology* (NIST)", Jurnal Sarjana Teknik Informatika, Vol 8, Nomor 2, Juni 2020, hal. 13.

[8] Vikran Fasyadhiyaksa Putra, "Modus Operandi Tindak Pidana Phising Menurut UU ITE", Jurnal Jurist Diction, Vol 4, Nomor 6, November 2021, hal. 2532.

[9] Nelson Tampubolon, *Bijak Ber-electronic Banking*, (Jakarta: Otoritas Jasa Keuangan,2015), hal. 48.

11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut "UU ITE") yang merujuk kepada tindakan seseorang dalam memanipulasi, atau menciptakan informasi elektronik palsu yang mirip dengan aslinya. Dalam metode ini, penipu akan mengarahkan nasabah kepada situs web dan surat elektronik palsu yang telah diciptakan dengan kemiripan yang persis dengan yang aslinya.[10]

Berdasarkan laporan yang disusun oleh Direktorat Tindak Pidana Siber Bareskrim Kepolisian Negara Republik Indonesia, jasa keuangan dijadikan sebagai incaran penyerangan *phising* terbesar di Indonesia dengan persentase sebanyak 41%.[11] Serangan *phising* akan mengelabui masyarakat dengan cara mencatut nama lembaga keuangan.[12] Banyak jasa keuangan yang menghimbau nasabah untuk tidak mudah percaya dengan penipuan mengatasnamakan suatu jasa keuangan yang disertai dengan penyebutan kode OTP (*One-Time Password*[13]). Kode OTP dijadikan sandi yang bersifat sementara guna melakukan verifikasi sebuah sistem.[14]

Penyebutan kode OTP dijadikan salah satu objek dalam *phising*. Kode OTP merupakan pin yang digunakan hanya sekali dalam mengakses sebuah sistem elektronik. Jika layanan keuangan difasilitasi dengan kode OTP, maka biasanya penipuan dilakukan dengan metode *phising.*[15] Jika seseorang memiliki atau

---

[10] Dian Rachmawati, "*Phising* Sebagai Salah Satu Bentuk Ancaman Dalam Dunia *Cyber*", Jurnal Ilmiah SAINTIKOM Sains dan Komputer, Vol 13, Nomor 3, September 2014, hal. 211.

[11] Cindy Mutia Annur, "Rawannya Perlindungan Data Pribadi di Indonesia", <https://katadata.co.id/ariayudhistira/infografik/6306f43b1e8b9/rawannya-perlindungan-data-pribadi-di-indonesia>, diakses 28 Agustus 2022.

[12] Teti Purwanti, *Op. Cit.*

[13] Law Insider, "*One Time Password definition*", <https://www.lawinsider.com/dictionary/one-time-password>, diakses pada 28 Agustus 2022.

[14] *Ibid.*

[15] Muhammad Sulthon Alif dan Ahmad R. Pratama, "Analisis Kesadaran Keamanan di Kalangan Pengguna *E-Wallet* di Indonesia", Skripsi, Yogyakarta: Universitas Islam Indonesia, Januari 2021, hal. 2.

mengetahui kode OTP ini, ia dapat saja mengakses sebuah akun meskipun bukan pemilik akun aslinya.[16] Usaha penipu dalam memperoleh kode OTP tersebut, yaitu mengirimkan pesan disertai desakan kepada nasabah terkait kode OTP untuk mengakses web[17] palsu yang telah diciptakan.[18] Selain identitas nasabah seperti nama, tanggal lahir, dan lainnya, kode OTP juga merupakan data elektronik yang wajib untuk dirahasiakan. Kode OTP menjadi kunci untuk mengakses sebuah sistem yang juga merupakan kumpulan dari data elektronik sebagaimana telah dinyatakan dalam Pasal 1 angka 8 dan 30 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut dengan "PP PSTE"). Oleh sebab itu, bank memiliki peran untuk memberikan himbauan terkait kerahasiaan kode OTP sebagai data pribadi.

Terdapat kasus *phising* yang terjadi pada beberapa bank di Indonesia. Pada bulan Agustus 2022, seorang pelaku penipuan mengatasnamakan PT Bank Central Asia, Tbk. (BCA) yang mengarahkan korban menuju situs palsunya.[19] Korban diminta untuk menyebutkan data pribadinya dengan iming-iming membantu korban.[20] Data pribadi biasanya meliputi pin, kode OTP, nomor kartu debit atau kredit dan informasi lainnya. Menyikapi penipuan ini, nasabah dihimbau untuk

---

[16] Eko Listiyani, "Kepastian Hukum Data Pribadi terkait *One Time Password* (OTP) dalam Penggunaan Media Elektronik", Skripsi, Surabaya: Fakultas Ilmu Sosial dan Hukum Universitas Negeri Surabaya, 2019, hal. 4.

[17] Kemendikbud, *KBBI Daring*, <https://kbbi.kemdikbud.go.id/entri/web>, diakses pada 8 November 2022.

[18] Nelson Tampubolon, *Op. Cit*, hal. 53.

[19] Noverius Laoli, "Waspada! Modus Penipuan Kenaikan Tarif Transaksi Rp 150.000 Intai Nasabah BCA dan BRI", <https://keuangan.kontan.co.id/news/waspada-modus-penipuan-kenaikan-tarif-transaksi-rp-150000-intai-nasabah-bca-dan-bri>, diakses 28 Agustus 2022.

[20] #AwasModusBCA, "Hati-Hati Pembajakan Akun Bank melalui *Phishing*", <https://www.bca.co.id/id/informasi/awas-modus/2022/07/22/08/18/hati-hati-pembajakan-akun-bank-melalui-phishing>, diakses 27 Agustus 2022.

lebih berhati-hati dan segera melakukan laporan baik melalui situs resmi pemerintah atau *call center* resmi BCA.[21] Selain itu terdapat juga kasus lain yang terjadi pada bulan Mei 2022. Seorang korban merupakan nasabah PT Bank Rakyat Indonesia Tbk (BRI) di Kota Padang, Sumatera Barat. Korban dikirimkan sebuah situs web yang persis dengan milik BRI serta dimintakan untuk mendaftarkan diri dengan mengisi data pribadinya dalam situs tersebut. Korban juga diminta menyebutkan kode OTP sebagai bentuk verifikasi dari BRI. Tidak lama kemudian, dalam mutasi rekeningnya korban telah melakukan transaksi sebesar Rp250.000.000 (dua ratus lima puluh juta Rupiah) dan transaksi lainnya. Korban mengaku telah mengalami kerugian dengan total lebih dari Rp1.100.000.000 (satu miliar seratus juta Rupiah).[22] Tidak hanya itu, seorang warga kabupaten Trenggalek, Sumatera Selatan merupakan nasabah BRI juga yang mengalami kerugian sebesar Rp84.000.000 (delapan puluh empat juta Rupiah). Kerugian yang dialaminya berasal dari kelalaian dalam memberikan data lengkapnya untuk melakukan verifikasi data dari *call center* palsu. Tidak lama kemudian, korban melaporkan kejadiannya ke pihak kepolisian dan pelaku berhasil diamankan. Pelaku penipuan mengaku sudah sering melakukan tindakan memanipulasi sebagai *call center* palsu.[23]

[21] *Ibid.*
[22] Riki Chandra, "Usut Kasus *Phishing* Nasabah BRI di Padang yang Rugi Miliaran Rupiah, Polisi: Kasus Ini Sudah Sering Terjadi", <https://sumbar.suara.com/read/2022/06/15/201500/usut-kasus-phishing-nasabah-bri-di-padang-yang-rugi-miliaran-rupiah-polisi-kasus-ini-sudah-sering-terjadi?page=all>, diakses 27 Agustus 2022.
[23] Aflahul Abidin, "Terungkap, Inilah Sosok di Balik *Call Center* BRI Palsu yang Menipu Nasabah Bank", <https://mataraman.tribunnews.com/2022/04/25/terungkap-inilah-sosok-di-balik-call-center-bri-palsu-yang-menipu-nasabah-bank?page=2>, diakses 29 Agustus 2022.

Melalui pemaparan beberapa kasus di atas, dapat dikatakan bahwa *phising* dilakukan melalui tindakan manipulasi atau berpura-pura menjadi *call center* palsu suatu bank bertujuan mengelabui nasabah agar menyebutkan data pribadinya yang meliputi kode OTP. Data pribadi ini berguna untuk melakukan verifikasi menuju akun sehingga dapat mengakses dana milik korban. Pemilik data pribadi seharusnya memahami bahwa kerahasiaan data pribadi tidak dapat dibagikan kepada orang lain dengan sembarangan. Hal ini diperjelas oleh Mariam Barata selaku Direktur Tata Kelola Ditjen Aptika bahwa kebocoran data pribadi juga seringkali disebabkan oleh kecerobohan dalam menjaga kerahasiaan pemilik data pribadinya sendiri.[24]

Pemerintah telah mengatur pengawasan terhadap bank dalam rangka pencegahan *phising* ini. Terdapat kewajiban berupa pemberian edukasi yang dilakukan bank sebagaimana diatur dalam Pasal 9 Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen Dan Masyarakat di Sektor Jasa Keuangan (selanjutnya disebut dengan POJK PKM SJK). Bank dapat memberikan edukasi yang salah satunya terkait mekanisme layanan jasa keuangan. Pelayanan berupa edukasi ini dinilai penting karena teknologi bersifat dinamis serta kompleksnya *digital savvy* mengenai data apa saja yang wajib untuk dirahasiakan.

OJK juga telah menetapkan standar yang harus dipenuhi bank selaku jasa keuangan terkait penerapan manajemen risiko keamanan siber. OJK melakukan peninjauan kebijakan yang berhubungan dengan pengelolaan, pelaksanaan,

[24] Pratiwi Agustini, "34 Persen Pelanggaran Data Pribadi akibat *Human Error*", <https://aptika.kominfo.go.id/2020/08/34-persen-pelanggaran-data-pribadi-akibat-human-error/>, diakses 30 Agustus 2022.

pengujian keamanan siber yang dapat diimplementasikan dalam sistem jasa keuangan di Indonesia.[25] Standar ini tertuang pada *consultative paper* untuk memberikan penerangan kepada bank terkait manajemen risiko keamanan siber. Salah satu penjelasan yang diberikan ini dapat terlihat di mana bank harus memastikan seluruh karyawan menerapkan dan mengerti kebijakan keamanan siber.[26] Pemahaman terkait kebijakan keamanan siber ini berhubungan dengan kewaspadaan dan pencegahan *phising*. Dalam penerapannya, penilaian karyawan dapat terlihat dari respon dan perilaku saat bank memberikan simulasi *phising.*

Bank memiliki kewajiban dalam mencegah *phising*. Pemenuhan kewajiban ini berada di bawah pengawasan oleh OJK dengan lembaga lainnya sebagaimana diatur pada POJK PKM SJK. Pengaturan ini telah dilaksanakan oleh salah satu aplikasi perbankan dari PT Bank Tabungan Pensiunan Nasional, Tbk. (BTPN) yang bernama Jenius dan berada di bawah pengawasan OJK dan Bank Indonesia. Program Jenius Aman ini ditujukan khusus untuk menghindari *phising,* melalui pengamanan data secara berlapis. Dalam pengaturan sistemnya, dilakukan memasukkan kode OTP secara berulang-ulang untuk melakukan verifikasi.[27] Pengaturan ini bertujuan untuk memastikan pihak yang memasukan kode OTP tersebut adalah nasabah sendiri selaku pemilik akun. Melalui program keamanan

[25] Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan, "*Consultative Paper*: Manajemen Risiko Keamanan Siber Bank Umum", <https://ojk.go.id/id/kanal/perbankan/implementasi-basel/Documents/Pages/Consultative-Papers/Consultative%20Paper%20Manajemen%20Risiko%20Keamanan%20Siber%20Bank%20Umum.pdf>, diakses pada 31 Agustus 2022.
[26] *Ibid.*
[27] Claudia Von Nasution, "Jenius Aman: Cara Jenius Jaga Keamanan", <https://www.jenius.com/highlight/detail/jenius-aman-cara-jenius-jaga-keamanan>, diakses pada 4 September 2022.

siber ini, Jenius sudah melaksanakan tanggung jawabnya sesuai dengan Pasal 6 POJK PKM SJK dalam melakukan pencegahan *phising* terhadap nasabah.

Dalam pemenuhan tanggung jawab bank terkait pencegahan serangan *phising* terhadap nasabahnya, beberapa bank menerapkan kebijakan guna peningkatan kualitas pelayanan. BTPN sendiri telah menerapkan kebijakan terkait pencegahan penipuan *call center* palsu melalui penentuan *Relationship Manager* tiap nasabah. Nasabah difasilitasi *Relationship Manager* beserta dengan kontak nomornya yang dikhususkan untuk membantu kebutuhan perbankan nasabah.[28] Kebijakan BTPN ini sangat berguna untuk mencegah nasabah yang berpotensi dihubungi *call center* palsu, karena nasabah telah memiliki kontak langsung dengan *Relationship Manager* tiap nasabah sendiri. Tidak hanya BTPN, BCA juga membuat sebuah program yang bertujuan untuk pengamanan data dalam sistemnya. Program *Data Loss Prevention* dijadikan strategi untuk mengamankan akses dari pelaku *phising*. BCA menerapkan sistem *Two Factor Authentication* yang bertujuan untuk melakukan verifikasi secara berulang untuk memastikan bahwa sistemnya diakses oleh nasabahnya sendiri. BCA juga memberikan latihan secara berkala yang bertujuan untuk meningkatkan rasa kewaspadaan pekerjanya dengan *e-mail phising test*.[29] Melalui penjelasan beberapa bank ini, terlihat adanya tanggung jawab dari bank selaku penyelenggara transaksi elektronik sebagai bentuk pencegahan penyerangan *phising*.

[28] BTPN, "Ikuti tips berikut untuk menjaga kenyamanan & keamanan aktivitas perbankan Anda", <https://www.youtube.com/watch?v=96DX-b1Vu20>, diakses pada 9 September 2022.
[29] PT Bank Central Asia Tbk, "Laporan Berkelanjutan 2020", <https://www.bca.co.id/-/media/Feature/Report/File/Sustainability-Index/SASB/SASB-FNCB230a1-1-Jumlah-pelanggaran-data-2-persentase-yang-melibatkan-informasi-identitas-pribadi-PI.pdf>, diakses pada 9 September 2022.

Pada lembaga pemerintah, Kemenkominfo dengan programnya yang melakukan kerja sama dengan Gerakan Nasional Literasi Digital (GNLD) Siberkreasi sebagai wadah dalam memberikan literasi digital kepada seluruh masyarakat meliputi nasabah dan bank. Edukasi ini dilakukan secara berkala dan tidak hanya secara khusus membahas mengenai kasus *phising* saja. Tidak hanya itu, terdapat sebuah akun Instagram resmi dari Kemenkominfo yang bernama *@misslambehoaks*[30]. Akun ini dikhususkan untuk memberikan klarifikasi terkait beredarnya sebuah berita yang membutuhkan kepastian akan kebenarannya. Dalam akun ini, penipuan *call center* palsu di sektor perbankan sering diunggah yang telah dikonfirmasi terlebih dahulu dengan bank terkait. Melalui kedua program yang dilakukan oleh Kemenkominfo ini, terlihat adanya usaha dalam mengatasi kasus ini namun masih belum dapat sepenuhnya tercapai.

Koordinasi antara OJK dan Kemenkominfo dapat membantu memperkuat perlindungan nasabah agar terhindar dari serangan *phising*. Koordinasi ini berguna untuk mempertahankan kedaulatan data dan pertahanan bagi nasabah terkait serangan *phising*.[31] OJK berperan dalam melakukan pengawasan terhadap tanggung jawab bank terkait keamanan siber sebagaimana diatur dalam Pasal 56 POJK PKM SJK. Kemenkominfo berperan dalam membuat kebijakan mengenai sistem transaksi elektronik. Kemenkominfo berkoordinasi dengan OJK yang

[30] LAMBE HOAKS, <https://www.instagram.com/misslambehoaks/>, diakses pada 8 November 2022.

[31] Otoritas Jasa Keuangan, "OJK dan Kominfo Perkuat Sinergi Pelayanan dan Perlindungan Masyarakat di Ruang Digital", <https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/OJK-dan-Kominfo-Perkuat-Sinergi-Pelayanan-dan-Perlindungan-Masyarakat-di-Ruang-Digital.aspx>, diakses pada 9 September 2022.

sejalan dengan pelaksanaan Pasal 34 ayat 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (selanjutnya disebut dengan "Permenkominfo PDPSE"). Oleh sebab itu, dalam kasus *phising* ini koordinasi antara OJK dan Kemenkominfo sebagai penegak hukum memiliki pengaruh dalam mencegah serta meningkatkan perlindungan data pribadi nasabah melalui sistem elektronik dari serangan *phising*.

Phising pada sektor perbankan dapat dicegah melalui pengetahuan, kewaspadaan, dan penerapan kebijakan. Bank memiliki peran penting dalam memberikan himbauan terkait *phising*. Bank wajib memberikan pemberitahuan dan pemahaman tentang *phising.*[32] Penerapan kebijakan yang ditujukan kepada masyarakat ini menjadi bentuk tanggung jawab perbankan. Penerapan kebijakan yang dilakukan bank dapat berupa pembaruan sistem elektronik terkait proteksi data nasabah, atau pun kebijakan dalam manajemen bank. Dengan diterapkan kebijakan oleh bank, terdapat pemenuhan tanggung jawab bank dalam keamanan nasabah terhadap risiko penyerangan *phising*.

Dari pemaparan yang telah dijabarkan penulis, penulis akan melakukan penelitian serta pendalaman materi dalam bentuk skripsi terhadap pencegahan serangan *phising* pada sektor perbankan meliputi bentuk koordinasi antara OJK dengan Kemenkominfo terhadap pelaku usaha dalam melakukan pencegahan serta tanggung jawab dari bank terhadap nasabahnya.

[32] Ikhsan Radiansyah, Candiwan, Yudi Priyadi, "Analisis Ancaman *Phishing* dalam Layanan Online Banking", Jurnal Ekonomika-Bisnis, Vol 7, Nomor 1, Januari 2016, hal. 8.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, terdapat rumusan masalah yang akan dibahas dalam penulisan skripsi ini yaitu:

1. Bagaimana regulasi yang mencakup koordinasi antara OJK dan Kemenkominfo terkait pencegahan *phising* pada nasabah?
2. Bagaimana tanggung jawab bank terkait pencegahan *phising* terhadap nasabah?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang disusun, maka tujuan yang ingin dicapai dalam penulisan skripsi ini adalah:

1. Menganalisis regulasi koordinasi OJK dan Kemenkominfo terkait pencegahan *phising* terhadap nasabah.
2. Meninjau persoalan hukum terkait tanggung jawab bank terkait pencegahan *phising* terhadap nasabah.

1.4 Manfaat Penelitian

Melalui penelitian ini, penulisan skripsi ini dapat memberikan memberikan manfaat kepada seluruh masyarakat Indonesia dalam melakukan pencegahan *phising* di sektor perbankan antara lain:

1.4.1 Manfaat Teoritis

Penulis berharap penulisan skripsi ini dapat memberikan pengetahuan tambahan atau bahan pustaka terkait dengan tindakan yang dilakukan oleh OJK dengan Kemenkominfo sebagai bentuk pencegahan *phising* terhadap nasabah.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan dukungan terhadap masyarakat yang berusaha untuk terhindar serangan *phising*, para pejabat sebagai pembuat kebijakan, dan bank terkait dengan tanggung jawabnya dalam pencegahan *phising*.

1.5 Sistematika Penulisan

Sistematika yang digunakan dalam penulisan skripsi ini terbagi atas 5 (lima) bab yang secara singkat akan memuat materi-materi dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan dimuat mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, sistematika penulisan sebagai bahan dasar penelitian dalam penulisan skripsi ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini, akan termuat tinjauan teori perlindungan hukum dan teori keamanan siber sebagai landasan penelitian. Melalui tinjauan teori yang disusun, akan dihubungkan dengan kebutuhan penelitian sebagai tinjauan konseptual terkait peran bank, OJK dan Kemenkominfo terkait pencegahan *phising*.

BAB III METODE PENELITIAN

Dalam bab ini akan dimuat metode penelitian yang digunakan sebagai pemecahan masalah penelitian skripsi ini. Pada bab ini akan dijelaskan jenis penelitian, data penelitian, teknik pengumpulan data, pendekatan penelitian, dan teknik analisis data untuk menunjang penelitian skripsi ini.

BAB IV HASIL PENELITIAN DAN ANALISIS

Dalam bab ini termuat penjelasan sebagai jawaban atas rumusan masalah yang disusun melalui teori-teori yang digunakan pada tinjauan pustaka.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan termuat kesimpulan atas hasil penelitian yang didapatkan dan saran atas permasalahan dalam penulisan skripsi ini.