Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter

Tesis S2

Progam Magister Akuntansi

Diajukan Oleh

Rahmadani Ningtyas Sekar Putri (20919008)

PROGRAM STUDI MAGISTER AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

2022

HALAMAN PERSETUJUAN

Yogyakarta, 16 September 2022

Telah diterima dan disetujui dengan baik oleh

Pembimbing,

Hendi Yogi Prabowo, SE., M.ForAcc., Ph.D.

BERITA ACARA UJIAN TESIS

Pada hari Senin tanggal 10 Oktober 2022 Program Studi Akuntansi Program Magister, Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia telah mengadakan ujian tesis yang disusun oleh:

RAHMADANI NINGTYAS SEKAR PUTRI

No. Mhs. : 20919008

Konsentrasi : Audit Forensik

Dengan Judul:

ANALISA POLA – POLA SOSIALISASI PENCEGAHAN MODUS SOCIAL ENGINEERINGOLEH BANK MELALUI MEDIA WEBSITE DAN MEDIA SOSIAL TWITTER

Berdasarkan penilaian yang diberikan
oleh Tim Penguji,maka tesis tersebut
dinyatakan **LULUS**

Penguji I	Penguji II
Hendi Yogi Prabowo, SE., M.ForAcc., Ph.D.	Dr. Kumalahadi, MS., Ak.

Mengetahui
Ketua Program Studi,

Arief Rahman, SE., SIP., M.Com., Ph.D.

HALAMAN PENGESAHAN

Yogyakarta, 17 Oktober 2022

Telah diterima dan disetujui dengan baik oleh :

Dosen Pembimbing

Hendi Yogi Prabowo, SE., M.ForAcc., Ph.D.

HALAMAN PERSEMBAHAN

Tesis ini peneliti persembahkan untuk suami, orang tua, keluarga, dan teman yang telah memberikan dukungan kepada peneliti, sehingga dapat menyelesaikan studi jenjang Magister.

KATA PENGANTAR

Bismillahirrahmanirrahim.

Alhamdulillah segala puji dan syukur penulis panjaykan kehadirat Allah Subhanahu wa Ta'ala yang telah melimpahkan segala rahmat-Nya dan kepada Nabi Muhammad Shallallahu'alaihi wa Sallam, karena nikmat-Nya sehingga penulis bisa menyelesaikan tesis dengan judul "Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter" yang merupakan sebuah karya ilmiah yang dibuat oleh penulis sebagai syarat dalam memenuhi tugas akhir di program studi Magister Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia.

Penulis menyadari bahwa tesis dapat diselesaikan berkat dukungan dan bantuan dari berbagai pihak, oleh karena itu penulis berterima kasih kepada semua pihak yang secara langsung maupun tidak langsung memberikan kontribusi dalam menyelesaikan tesis ini.

1. Prof. Fathul Wahid, S.T., M.Sc., Ph.D. selaku Rektor di Universitas Islam Indonesia.

2. Bapak Johan Arifin, S.E., M.Si., Ph.D., CFrA. selaku Dekan Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia.

3. Bapak Drs. Dekar Urumsah, S.E., S.Si., M.Com.(IS)., Ph.D., CFrA selaku Ketua Jurusan Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, yang selalu memberikan motivasi dan dukungan, serta arahan kepada penulis.

4. Bapak Arief Rahman, S.E., S.I.P., M.Com., Ph.D. selaku Ketua Program Studi Magister Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia.

5. Bapak Hendi Yogi Prabowo, S.E., M.ForAcc., Ph.D. Selaku dosen pembimbing yang tanpa lelah telah memberikan bimbingan dan arahan kepada penulis sejak awal penelitian sampai terselesaikannya penelitian ini. Semoga Allah memberikan kebahagiaan dan pahala melimpah atas segala kebaikan dan bimbingan yang telah diberikan kepada penulis.

6. Seluruh dosen Magister Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia atas ilmu dan bimbingan yang diberikan, sehingga penulis dapat bertumbuh menjadi mahasiswa yang berilmu dan tangguh serta mengenal akuntansi dari aspek keislaman.

7. Bapak Sakimin dan Ibu Siti Komariah selaku kedua orang tua yang telah memberikan dukungan serta doa tulus, sehingga penulis dapat melalui segala rintangan selama studi.

8. Ajo Muhammad Hifzan Sadida selaku suami penulis yang telah memberikan perhatian, motivasi, serta doat tulus sehingga penulis semangat dalam melakukan penelitian penulisan ilmiah ini.

9. Terimakasih kepada Mas Riko dan Mas Adit selaku saudara penulis yang telah memberikan doa dan dukungan atas proses penelitian ini.

10. Terimakasih kepada seluruh Magister Akuntansi Angkatan 21 yang sudah menemani penulis selama proses pembelajaran dari awal sampai hari ini.

Penulis menyadari bahwa dalam penelitian ini belum sempurna. Oleh karena itu penulis berharap mendapatkan banyak masukan serta bimbingan dari pembaca terkait penelitian ini. Semoga Allah memberikan kemudahan dan petunjuk kepada penulis untuk dapat melaksanakan penelitian yang lebih baik. Hanya kepada Allah penulis memohon diberikan ilmu dan amal yang bermanfaat bagi dunia dan akhirat.

Bandarlampung, September 2022

Penulis

Rahmadani Ningtyas Sekar Putri

DAFTAR ISI

HALAMAN JUDUL……...i
HALAMAN PERSETUJUAN……...ii
BERITA ACARA……iii
HALAMAN PENGESAHAN...……iv
HALAMAN PERSEMBAHAN……v
KATA PENGANTAR……..vi
DAFTAR ISI……..……...ix
DAFTAR TABEL……xii
DAFTAR GAMBAR……..…xiii
ABSTRAK……..xiv
BAB 1 PENDAHULUAN……1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 12
1.3 Fokus Penelitian..... 14
1.4 Tujuan Penelitian 14
BAB II KAJIAN PUSTAKA..... 18
2.1 Pengenalan Bab……...18
2.2 Peta Literatur……...19
2.3 Consumer Fraud 20
2.4 Crime Triangle of Routine Activity Theory..... 21
2.5 Cybercrime 24
2.6 *Social Engineering Attacks*..... 27
2.6.1 Prinsip Serangan *Social Engineering* 30
2.6.2 Karakateristik Serangan *Social Engineering*..... 33
2.6.3 Bentuk Serangan *Social Engineering*..... 34
2.6.4 Faktor Penyebab *Social Engineering* 38
2.6.5 Ancaman *Social Engineering Attack* Bagi Nasabah 39
2.7 Gullibility..... 40
2.8 Strategi Sosialisasi..... 42

2.8.1 Website 43
2.8.2 Twitter 44
2.8.3 Whatsapp 45
2.8.4 Email 46
2.8.5 Instagram 47
2.8.6 Call Center 48
2.9 Penelitian Terdahulu 48
BAB III METODE PENELITIAN 53
3.1 Pengenalan Bab 53
3.2 Alasan Memilih Penelitian Kualitatif 53
3.3 Desain Penelitian 54
3.4 Rancangan dan Tahapan Penelitian 55
3.4.1 Tahap Penentuan Topik Penelitian 57
3.4.2 Tahap Penentuan Rumusan Masalah 57
3.4.3 Tahap Pengumpulan Data 58
3.4.4 Tahapan Analisis Data 59
3.4.5 Interpretasi Data 67
3.5 Objek Penelitian 67
3.6 Instrumen Penelitian 67
3.7 Pengujian Keabsahan Data 68
3.7.1 Uji Kredibilitas 68
3.7.2 Uji Dependabilitas 70
BAB IV HASIL DAN PEMBAHASAN 71
4.1 Pengenalan Bab 71
4.2 Gambaran Umum Perusahaan Perbankan di Indonesia 72
4.2.1 PT. Bank Mandiri (Persero) Tbk 72
4.2.2 PT. Bank Central Asia Tbk. 75
4.2.3 PT. Bank Rakyat Indonesia (Persero) Tbk. 77
4.2.4 PT. Bank Negara Indonesia (Persero) Tbk 79
4.2.5 PT. Bank Permata Tbk 81
4.2.6 PT. Bank Syariah Indonesia Tbk 83
4.3 Gambaran Permasalahan Penipuan *Social Engineering* Pada Nasabah Bank - Bank Yang Terdapat Di Indonesia 87

4.3.1 Crime Triangle *94*

4.3.2 Social Engineering Attacks *123*

4.4 Pola – Pola Strategi Sosialisasi Pencegahan Penipuan *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter 135

4.4.1 Website 137

4.4.2 Twitter..... 155

4.5 Kekurangan Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* di Media Website dan Media Sosial Twitter..... 171

4.5.1 Kekurangan Pada Sosialisasi Melalui Media Website..... 171

4.5.2 Kekurangan Pada Sosialisasi Melalui Media Twitter..... 173

4.6 Perbaikan yang Dapat Dilakukan Bank Dalam Sosialisasi Pencegahan Penipuan *Social Engineering*……175

4.6.1 Perbaikan yang Dapat Dilakukan Bank Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Media Website..... 176

4.6.2 Perbaikan yang Dapat Dilakukan Bank Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Media Twitter..... 178

BAB V KESIMPULAN 180

5.1 Pengenalan Bab..... 180

5.2 Kesimpulan..... 180

5.3 Keterbatasan Penelitian 181

5.4 Saran..... 182

5.4.1 Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Syariah Indonesia (BSI), Bank Permata..... 182

5.4.2 Masyarakat..... 183

5.4.3 Penelitian Selanjutnya 183

DAFTAR PUSTAKA……184

DAFTAR TABEL

Tabel II. 1 Rangkuman Karakteristik Serangan Social Engineering..... 33
Tabel IV. 1 Matrix Coding Query Gambaran Permasalahan Penipuan *Social Engineering* (Berdasarkan Jumlah Kata) 93
Tabel IV. 2 *Matrix Coding* Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Website* (Berdasarkan Jumlah Kata) 139
Tabel IV. 3 Matrix Coding Query Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Twitter (Berdasarkan Jumlah Kata)..... 157

DAFTAR GAMBAR

Gambar I.1 Data Pertumbuhan Digital Tahunan 2
Gambar II. 1 Peta Literatur Penelitian..... 19
Gambar II. 2 Crime Triangel of Routine Activity Theory 23
Gambar II. 3 Siklus Hidup Social Engineering..... 31
Gambar II. 4 Rumus Gullibility 41
Gambar III. 1 Tahap Penelitian..... 57
Gambar IV. 2 Struktur Organisasi PT. Bank Mandiri (Persero) Tbk..... 76
Gambar IV. 3 Struktur Organisasi PT. Bank Central Asia Tbk..... 78
Gambar IV. 4 Struktur Organisasi BRI 80
Gambar IV. 5 Struktur Organisasi BNI..... 82
Gambar IV. 6 Struktur Organisasi Bank Permata 84
Gambar IV. 7 Struktur Organisasi Bank Syariah Indonesia 86
Gambar IV. 8 Data Serangan Siber di Indonesia 88
Gambar IV. 9 Peta Analisa Pola – Pola Strategi Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Website 138
Gambar IV. 10 Akun Whatsapp Bank Palsu 146
Gambar IV. 11 Poster Sosialisasi Bank Permata Melalui Website..... 151
Gambar IV. 12 Peta Analisa Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Twitter* 156
Gambar IV. 13 Peta Analisa Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Twitter*..... 156
Gambar IV. 14 Postingan Twit Sosialisasi Bank Central Asia (BCA)..... 159
Gambar IV. 15 Sosialisasi Akun Palsu Whatsapp BCA Melalui Twitter 160
Gambar IV. 16 Twitter Sociogram BCA..... 161
Gambar IV. 17 Sosialisasi Langkah – Langkah Pencegahan Social Engineering Bank Mandiri Melalui Twitter..... 162
Gambar IV. 18 Poster Langkah – Langkah Pencegahan Penipuan BRI..... 164
Gambar IV. 19 Poster Ciri – Ciri Akun Instagram Palsu BRI 165
Gambar IV. 20 Sosialisasi Pencegahan Penipuan Melalui Twit BNI 166
Gambar IV. 21 Sosialisasi Akun Palsu BSI..... 167
Gambar IV. 22 Poster Ciri – Ciri Akun Palsu BSI..... 167
Gambar IV. 23 Sosialisasi Pencegahan Penipuan Bank Permata 168
Gambar IV. 24 Poster Sosialisasi Pencegahan Penipuan Bank Permata..... 169

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi pola – pola strategi sosialisasi pencegahan penipuan *social engineering* melalui media website dan media sosial twitter yang diberikan oleh enam bank besar di Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan menggunakan data sekunder yang sifatnya dokumen, peneliti menggunakan situs website resmi dan media sosial twitter milik bank sebagai media untuk mengumpulkan data. Data diambil menggunakan tool *NCapture* untuk men-*capture* konten yang terdapat di media website dan media sosial twitter. Hasil penelitian menunjukkan bahwa keenam bank memiliki pola sosialisasi pencegahan penipuan yang berbeda – beda pada media website dan media twitter yang memuat informasi sosialisasi mengenai ciri – ciri penipuan, layanan sarana kontak, dan langkah – langkah pencegahan penipuan *social engineering*.

BAB I

PENDAHULUAN

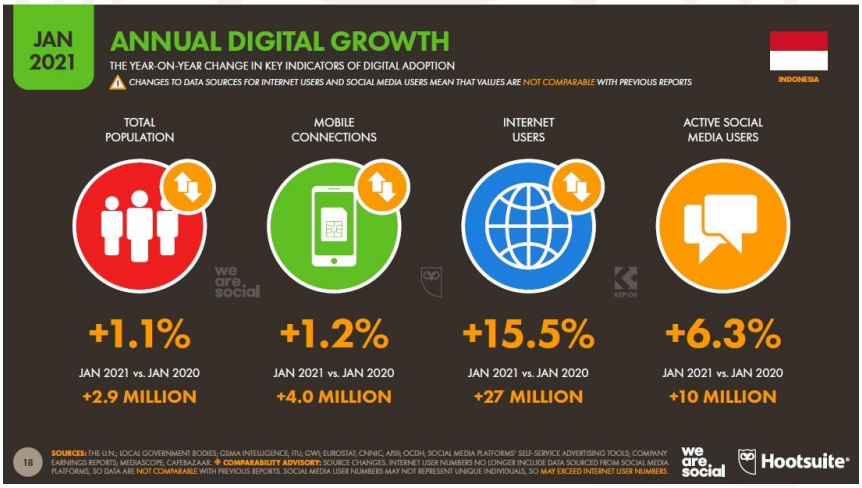
1.1 Latar Belakang Masalah

Perkembangan teknologi informasi memiliki berbagai manfaat dalam berbagai sector terutama sector perbankan. Penggunaan teknologi informasi pada sector perbankan dapat memudahkan perusahaan perbankan dalam memberikan pelayanan pada nasabah. Dewasa ini kehadiran teknologi informasi dapat membuka peluang bisnis yang baru, dan menciptakan lapangan pekerjaan. Teknologi informasi yang menjadi kebutuhan di dunia ini salah satunya adalah internet, berbeda hal nya dengan zaman dahulu internet hanya digunakan untuk penelitian akademis. Namun perkembangan internet sekarang sudah menjadi primadona di dunia, sehingga internet dapat digunakan dalam dunia bisnis yaitu dapat memberikan pelayanan dalam segi operasional.

Adanya pandemi *Covid*-19 telah merubah banyak hal termasuk aktivitas masyarakat yang mengharuskan melakukan semua pekerjaan dilakukan secara online sebagai bentuk mendukung gerakan tetap dirumah. Hal ini disebakan penerapan perarturan pembatasan skala besar (PSBB) yang mengharuskan masyarakat untuk *stay at home* dan *social distancing*. Kondisi seperti ini tentunya memiliki dampak ke sistem perekonomian bahkan di semua sektor, sehingga dengan keadaan ini membuat Indonesia harus mampu berjuang untuk mempertahankan perekonomian bangsa.

Pandemi Covid juga mengubah kebiasaan masyarakat yang biasa nya banyak dilakukan secara tatap muka, namun sekarang dilakukan secara online. Sebagai contohnya jika ingin berbelanja kebutuhan dapat dilakukan secara online dan melakukan pembayaran pun secara online. Maka dari itu, sebagai lembaga keuangan, Bank yang ada di dunia dituntut untuk dapat berinovasi agar dapat meningkatkan kepercayaan masyarakat dengan menyediakan *e-banking*, *e-money*, *online payment point*, sms banking dan lain – lain untuk melakukan transaksi agar dapat memudahkan nasabah dalam melakukan transaksi dimana saja tanpa harus keluar rumah.

Gambar I.1 Data Pertumbuhan Digital Tahunan



Sumber : *Hootsuite* dan *We are Social* (2021)

Berdasarkan data dari *Hootsuite* dan *We are Social* (2021) menunjukkan bahwa per januari 2021 pengguna internet naik sebesar 27 juta atau 15,5% dari total populasi, yang persentase tersebut naik dari tahun sebelumnya. Selain itu, peningkatan pengguna media sosial yang aktif per januari tahun 2021 sebesar 10

juta atau 6,3% dari total populasi. Jadi dapat disimpulkan bahwa penggunaan internet di dunia digital yang semakin meningkat, dan media sosial menjadi pilihan untuk memudahkan masyarakat dalam berinteraksi atau komunikasi.

Cahyolaksono et al. (2021) mengatakan terdapat studi yang dilakukan East Venture Digital Competitiveness Index (EV-DCI) 2021 yang menunjukkan bahwa semakin merata persaingan dunia digital antar provinsi di Indonesia. Hal ini ditunjukkan kenaikan skor median indeks daya saing digital (EV-DCI) pada tahun 2020 sebesar 27,9 yang kini pada tahun 2021 naik menjadi 32,1. Mengatakan terdapat dua faktor yang mendorong Indonesia mengalami perkembangan dan pemerataan daya saing digital di Indonesia yaitu pembangunan infrastruktur yang semakin merata. Hal ini ditunjukkan skor tertinggi menurut EV-DCL dari 7,5 point menjadi 54,3 pada tahun 2021.

Faktor yang kedua yaitu penggunaan teknologi informasi dan komunikasi (TIK) yang semakin meningkat. Hal ini ditandai dengan kenaikan pada pengeluaran TIK menurut EV-DCL sebesar 6,3 point pada tahun 2021. Hal ini dapat terjadi karena masa pandemic COVID -19 yang mengharuskan masyarakat untuk *work from home* (WFH) sehingga penggunaan TIK menjadi bagian penting di setiap aktivitas masyarakat.

Data Bank Indonesia menunjukkan bahwa transaksi pembayaran dengan menggunakan digital payment meningkat setiap tahun nya. Pada bulan September 2021 data dari Bank Indonesia (2021) menunjukkan jumlah uang eletronik yang

beredar terdapat 530.664.510 transaksi sedangkan dapat dibandingkan dengan September tahun 2020 hanya 393.904.001 transkasi.

Teknologi yang semakin berkembang membuat semua orang untuk dapat mengikuti zaman yang serba online. Sehingga keberadaan teknologi informasi di tengah masyarakat tidak dapat dipisahkan dengan internet. Penggunaan internet di zaman sekarang tidak selalu dari sisi positif saja namun penggunaan internet juga memiliki dampak negative. Keberadaan internet membuat pengguna nya harus berhati – hati karena jaringan internet rentan terhadap penipuan *(fraud)* yang hal ini termasuk kejahatan siber.

Gibbs (2020) mengatakan kerentanan *cyber crime* yang meningkat disebabkan pesat nya perkembangan teknologi. Tindakan penipuan *(fraud)* memang tidak bisa dijauhkan dari perkembangan teknologi, karena semakin berkembangnya teknologi maka semakin beragam juga kejahatan penipuan di dunia perbankan. Selain itu setiap keuntungan dan kemudahan yang diperoleh, maka terdapat pula kerugian dan kelemahan yang di dapatkan dari teknologi. Kelemahan tersebut yaitu munculnya tindakan kejahatan Informasi dan Transaksi Elektronik (ITE) atau *cybercrime* seperti kasus *phising, hacking, carding, skimming,* dan lain nya. Muncul nya masalah baru ketika semua aktivitas sehari –hari melibatkan system internet yaitu adanya tindakan kriminal berbasis (*cyber crime*) yang dilakukan oleh beberapa pihak yang berusaha memanfaatkan kelemahan sistem dan kesadaran pengguna terhadap sistem informasi..

Cyber crime merupakan tindakan kejahatan di dunia maya dengan bantuan alat komputer yang aktivitas tersebut banyak menggunakan jaringan internet. Menurut Ali (2019) *frauder* dapat melakukan berbagai kejahatan dengan teknik dan metode yang berbeda di dunia maya khususnya di dunia perbankan seperti *phising*, *vishing*, mengindetifikasi pencurian, penolakan layanan, rekayasa social, dan lain nya yang bertujuan untuk mencuri data keuangan nasabah.

Hingga saat ini, perbankan terus menerus melakukan pengembangan *online banking* yang tentu saja sangat membutuhkan internet. Sektor perbankan merupakan salah satu target utama oleh para pelaku kecurangan. Dunia perbankan sangat rentan dengan penipuan karena di sektor perbankan banyak melakukan transaksi keuangan.

Selain itu sering terdengar berita bahwa terdapat yang melapor ke polisi atas tindakan penipuan dengan modus yang sudah di organisir khususnya di sektor perbankan. Hal ini disebabkan karena adanya kemajuan teknologi yang dapat memudahkan untuk bertransaksi, sehingga semakin mudah *fraude*r untuk melakukan penipuan. Berdasarkan berita dari media cetak maupun online sebagian besar *fraud* yang terjadi disebabkan kelalaian dan kurang nya pemahaman dari konsumen sebagai pemegang informasi data keuangan nya sendiri.

Dalam penyerangan ini umumnya pelaku melakukan aksinya di belakang komputer atau dapat juga menghampiri targetnya secara langsung sebagai upaya untuk menambah kepercayaan target untuk mendapatkan informasi yang penting dengan cara mempengaruhi psikologi target dan mengeksploitasi kelemahan –

kelemahan dari sebuah keamanan. Jaringan keamanan manusia menjadi bagian yang terlemah dalam sebuah sistem tersebut, seperti hal nya manusia yang telah menjadi korban penyerangan tidak menyadari kalau sedang ditipu, karena korban telah dipengaruhi secara halus supaya mau mengikuti perintah dari pelaku penyerangan.

Oleh karena itu sangat perlu untuk menjadikan manusia sebagai prioritas yang harus diamankan, sebab manusia atau *user* dalam kasus ini sebagai jembatan bagi pelaku penyerangan untuk mendapatkan akses ke dalam sistem tersebut. Walaupun terdapat dinding pengamanan yang telah terpasang, hal ini tidak menjadi penghalang bagi pelaku penyerangan, karena pelaku penyerangan telah membuat strategi untuk mengakses sistem yang telah terlindungi. Jenis serangan *cyber crime* ini yang disebut *social engineering.*

Banyak ancaman yang ditimbulkan dari serangan *social engineering* yang diperkuat dengan data – data berupa contoh kasus yang telah terjadi sebelumnya. Contoh kasus ini dapat dijadikan sebagai tolak ukur akan ancaman yang ditimbulkan oleh *social engineering.* Sebagai contoh kasus serangan *social engineering* yang telah melegenda yaitu kasus Kevin Mitnick.

Kevin Mitnick merupakan seorang *hacker* yang sebagian besar teknik yang dilakukan adalah teknik *social engineering* yang melakukan aksinya hampir tanpa menggunakan komputer, namun kevin melakukan aksinya dengan cara mengeksploitasi kelemahan targetnya. Saat itu, Kevin Mitnick terbukti masuk ke beberapa sistem komputer milik perusahaan ternama yang kemudian mencuri

software – *software* miliki perusahaan tersebut. Perusahaan tersebut diantaranya Motorola, Novell, Fujitsu, Sun Microsystems, dan perusahaan lainnya. Salah satu tindakan kriminal lainnya yang dilakukan oleh Kevin adalah mencuri email dan berpura – pura menjadi karyawan perusahaan Nokia, lalu mencuri *software* yang sedang dikembangkan oleh perusahaan tersebut.

Selain itu pada tahun 2016 terdapat kasus penipuan yang menyeret 2 perusahaan besar yang ada di Indonesia. Melalui berita lewat Kompas.com Kartika Dewi (2020) menuliskan berita terdapat kasus yang menimpa dokter gigi di Surabaya, yang saat itu menjadi korban pembobolan rekening dan uang yang hilang sekitar Rp. 400.000.000.

Dokter gigi ini mengisahkan kasus nya bermula dari telepon yang diterimanya dari seseorang yang mengaku dari salah satu bank di Indonesia tempat dokter gigi ini menabung. Saat itu, dokter gigi ini menerima teleponnya dan pada akhirnya merasa terganggu sehingga dokter gigi ini menutup teleponnya. Namun, setelah menutup teleponnya dokter gigi mengetahui isi rekening tabungan nya hanya terdapat Rp. 500.000 yang awalnya Rp. 400 juta. Kasus ini pun menyeret dua perusahaan besar yaitu salah satu perusahaan telekomunikasi yang digunakan oleh dokter gigi untuk nomor ponselnya dan bank tempat menyimpan uangnya.

Berdasarkan pengamat teknologi informasi (TI) Ruby Alamsyah mengatakan kasus ini termasuk kasus penipuan yang bermodus *phising* yang kemungkinan besar dapat diakses melalui *email* korban. Modus penipuan dengan teknik *phising* ini, penyerang menglabui korban secara psikis yang bertujuan untuk mencuri akun

korban. Dalam kasus ini penyerang tidak hanya meretas akun korban yang ada di internet, namun penyerang juga melakukan transaksi dengan mentransfer dana yang ada di rekening korban.

Berdasarkan contoh kasus diatas dapat dikatakan bahwa dalam teknik *social engineering,* seorang penyerang akan berusaha mengajak *user* yang memiliki akses atas informasi atas perusahaan mau memberikan *username* dan *password* karyawan tersebut, dan seringkali karyawan tidak menyadari bahwa dirinya telah menjadi korban. Setelah penyerang mendapatkan *username* dan *password,* maka penyerang dapat dengan mudah untuk masuk ke dalam sistem perusahaan dan seolah – olah penyerang memiliki hak akses yang resmi.

Sering sekali terjadi kasus – kasus penipuan ditambah disektor perbankan adalah sasaran utama bagi pelaku penipuan. Maka dari itu, tidak sedikit nasabah ketika menjadi korban penipuan menyalahkan pihak bank. Padahal dalam kasus ini nasabah atau pengguna aplikasi online turut bertanggung jawab atas kasus tersebut, karena salah satu nya faktor penyebab adalah pengetahuan yang minim dan kelalaian dari pengguna. Maka dari itu nasabah diperlukan untuk mengetahui modus kejahatan penipuan yang sering terjadi seperti :

- Mendapatkan hadiah undian melalui telepon

  Penipuan ini dilakukan oleh pelaku dengan modus memberikan hadiah atau memberikan iklan barang agar nasabah terpancing untuk mengikuti instruksi pelaku sehingga pada akhirnya pelaku penipuan akan memandu nasabah untuk mengirimkan uang lewat transfer. Penipuan semacam ini sering sekali terjadi,

terkhususnya pada orang tua yang kurang paham mengenai masalah seperti ini sehingga mudah untuk dilabui.

- Mendapatkan *email* dari "bank"

  Pelaku penipuan mengirimkan *email* ke nasabah dengan modusnya adalah meminta nasabah memasukkan nomor data diri, nomer rekening dan PIN dengan melalui website yang palsu namun seolah – olah mirip dengan website aslinya.

- Menawarkan investasi dengan pengembalian tinggi

  Kegiatan investasi merupakan suatu hal yang sudah umum dikalangan masyarakat, dengan investasi seseorang bisa meraih keuntungan yang didapat namun sebaliknya jika investasi tersebut memberikan janji akan mengembalikan dengan return yang tinggi maka hal ini perlu di waspadai karena dengan tawaran yang terlalu tinggi biasanya tidak data memenuhi janji mengenai imbalan hasil yang sudah ditentukan.

- Penipuan dengan kartu kredit di internet

  Perkembangan internet yang memudahkan nasabah untuk melakukan transaksi salah satu cara nya adalah dengan menggunakan kartu kredit internet. Penggunaan kartu kredit internet ini dengan memasukkan nomor kartu kredit, masa berlaku dan tiga digit kode rahasia yang umumnya terletak dibagian belakang kartu kredit. Namun tidak sedikit hal ini dapat dimanfaatkan oleh orang – orang yang tidak bertanggung jawab.

- Memalsukan nomor *call center* ATM

  Modus jenis ini sering dilakukan oleh pelaku dengan bermulai duduk dekat ATM untuk mengintai situasi yang selanjutnya membuat ATM seolah rusak dan menelan kartu nasabah. Kemudian pelaku akan menempelkan nomor call center palsu di

badan ATM. Nasabah yang diiringi dengan rasa panic, tanpa sadar akan menghubungi *call center* palsu tersebut, pelaku penipuan akan memandu nasabah untuk menyebutkan nomer PIN dengan alih alih dijanjikan ATM nya akan diganti dan dikirimkan. Namun sebetulnya pelaku penipuan sudah mengantongi kartu ATM dan menyimpan PIN ATM nasabah sehingga pelaku penipuan dapat menguras tabungan nasabah sewaktu – waktu.

Pada umumnya benteng keamanan yang paling utama adalah pribadi dari nasabah atau pengguna itu sendiri, karena semua informasi dan data rahasia dipegang oleh nasabah. Oleh karena itu, nasabah diperlukan untuk menjaga rahasia informasi dan tidak mudah percaya dengan pihak- pihak yang ingin meminta nya, lalu memiliki sikap kehati – hatian dalam arti selalu berwaspada ketika ingin melakukan transaksi.

Oleh karena itu, serangan kriminal jenis *social engineering* ini dapat menimbulkan kerugian dari berbagai pihak. Pihak nasabah yang dirugikan secara finansial, dan kerugian terbesar juga yang dialami oleh perusahaan perbankan yaitu jatuhnya corporate branding yang dibangun selama ini oleh perusahaan. Menurut Gangwani (2021) bank lebih retan dengan masalah penipuan, kejahatan di dunia maya, pencurian online yang hal ini dapat merusak reputasi bank itu sendiri. Oleh karena itu, bank harus menemukan cara untuk meningkatkan layanan yang lebih berkualitas dengan membuat strategi internet banking (Namahoot & Laohavichien, 2018).

Menurut Olowookere dan Adewale (2020) beberapa tindakan pencegahan yang dapat mengurangi *fraud* pada kasus perbankan yaitu memverifikasi chip dan PIN, aktivasi kartu, kode/nilai verifikasi kartu, dan layanan verifikasi alamat, cara ini dirancang untuk mengekang penipuan. Kejadian penipuan mengindikasikan bahwa *frauder* pintar dalam melewati langkah – langkah pencegahan, mekanisme deteksi sehingga dapat berhasil melakukan kecurangan. Sehingga diperlukan teknik pembelajaran teknologi yang canggih sebagai upaya mengurangi penipuan di sektor perbankan. Adanya pemahaman tentang teknologi informasi akan memudahkan untuk menyelidiki penipuan yang terkait dengan masalah komputer (Gangwani, 2021).

Hasan dan Febriany (2021) mengatakan maraknya perkembangan digital dan teknologi yang semakin canggih memiliki dampak positif dan juga negatif bagi dunia perbankan, dan semakin banyak juga kejahatan dari segi financial, sehingga diperlukan langkah pencegahan dan penganan. Maka dari itu diperlukan langkah – langkah mitigasi untuk mengatasi masalah diatas yaitu dilakukan pencegahan penipuan *(fraud)* dengan memberikan edukasi kepada nasabah dari pihak bank untuk menimalisir terjadinya penipuan.

Chevers (2019) mengatakan bahwa pemberian edukasi *cyber crime* dapat meningkatkan kewaspadaan terhadap kejahatan *cyber crime* seperti *phising*. Nasabah dan masyarakat akan diberikan bekal edukasi yang memadai supaya dapat mengenali modus – modus penipuan secara dini. Pemberian edukasi dapat melalui media sosial dan situs resmi perusahaan, sehingga dapat memudahkan para nasabah dan masyarakat dalam mengakses informasi tersebut.

Oleh karena itu, Penelitian ini dilakukan untuk memberikan pemahaman yang jelas kepada masyarakat mengenai *social engineering*, dengan berdasarkan tiga alasan yaitu

1. Pemahaman sebagian masyarakat Indonesia masih mengenal *hacker* hanya menggunakan komputer, namun saat ini penyerang memiliki banyak cara untuk mengakses sistem yang menjadi target sasaran tanpa menggunakan teknis khusus.
2. Masyarakat Indonesia sebagian besar belum paham tentang *social engineering* dan menganggap kasus ini merupakan kasus yang baru.
3. Meningkatkan kewaspadaan masyarakat dengan memberikan pemahaman yang jelas mengenai *social engineering* dan ancaman yang ditimbulkan nya.

Adanya pemahaman mengenai *social engineering* diharapkan masyarakat lebih waspada terhadap ancaman ini. Oleh karena itu, penelitian ini akan membahas mengenai Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter.

1.2 Rumusan Masalah

1. Bagaimana gambaran umum permasalahan penipuan *social engineering* pada nasabah bank - bank yang terdapat di Indonesia ?

- Pada rumusan masalah ini, peneliti mengidentifikasi penipuan yang terjadi pada nasabah perbankan yang terdapat di Indonesia yang bertujuan untuk memahami gambaran secara umum permasalahan penipuan *social engineering* terkait dengan disertai dengan macam – macam modus penipuan

nya. Adapun perusahaan perbankan yang akan dibahas dalam penelitian ini yaitu bank – bank yang memiliki aset besar yang tercatat oleh OJK dan Bank Indonesia per Februari 2022 diantaranya Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Syariah Indonesia (BSI), Bank Permata.

2. Bagaimana pola – pola strategi sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh bank melalui media website dan media sosial twitter ?

- Dalam rumusan masalah ini, peneliti mengidentifikasi pola – pola strategi sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh bank melalui media website dan media sosial twitter yang telah peneliti dapatkan menggunakan *tool NCapture* dari Software *NVivo*. Pada penelitian ini peneliti akan menganalisa sosialisasi yang diberikan oleh Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Syariah Indonesia (BSI), Bank Permata, yang menginformasikan mengenai ciri - ciri penipuan, layanan sarana kontak, serta langkah - langkah pencegahan penipuan.

3. Bagaimana perbaikan yang sebaiknya dilakukan oleh perusahaan perbankan dalam rangka peningkatan sosialisasi di media website dan media sosial twitter?

    - Dalam rumusan masalah ini, peneliti memberikan usulan mengenai perbaikan yang dapat dilakukan oleh perusahaan perbankan dalam rangka

peningkatakan edukasi yang diberikan kepada nasabah sebagai upaya pencegahan penipuan melalui website dan media sosial twitter.

1.3 Fokus Penelitian

Supaya informasi yang diperoleh relevan dan dapat menjawab rumusan masalah, maka dalam penelitian ini, peneliti memiliki fokus penelitian diantara nya :

1. Aspek penelitian : Mekanisme Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter.
2. Objek Penelitian : Media sosial twitter dan situs resmi (website) 6 perusahaan perbankan di Indonesia yaitu Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI).

1.4 Tujuan Penelitian

Setelah menguraikan latar belakang dan rumusan masalah, maka peneliti memiliki tujuan dalam penelitian ini, yaitu :

1. Untuk mengetahui bagaimana gambaran permasalahan penipuan *social engineering* pada nasabah perbankan yang terdapat di Indonesia.
2. Untuk mengetahui pola – pola strategi sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh bank melalui media website dan media sosial twitter.

3. Untuk mengetahui bagaimana perbaikan yang sebaiknya dilakukan oleh bank – bank di Indonesia dalam rangka peningkatakan sosialisasi di media website dan media sosial twitter.

1.1 Manfaat Penelitian

Pada penelitian ini, harapannya hasil akhir penelitian ini dapat bermanfaat :

1. Bagi dibidang akademik dan pihak lainnya yang membutuhkan untuk dijadikan sebagai referensi di masa datang dengan tema yang relevan atau kajian pembahasan mengenai strategi pencegahan penipuan *social engineering* pada nasabah bank.
2. Bagi peneliti dapat menambah wawasan dan pengetahuan yang berhubungan dengan strategi pencegahan penipuan *social engineering* pada nasabah bank melalui media website dan media sosial twitter.
3. Bagi perusahaan perbankan : Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI) dapat di jadikan masukan sebagai bahan evaluasi untuk melakukan perbaikan dalam rangka peningkatakan sosialisasi di media website dan media sosial twitter.

1.2 Sistematika Penulisan

Penelitian ini memiliki 5 bab, dengan sistematika penulisan penelitian sebagai berikut :

BAB I PENDAHULUAN

Bab ini memiliki pembahasan yang meliputi latar belakang dan rumusan masalah. Selain itu diuraikan pula tentang

fokus penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan pada penelitian ini.

BAB II KAJIAN PUSTAKA

Bab ini menyajikan teori – teori yang digunakan dalam penelitian sebagai acuan berfikir dan menganalisis, serta memaparkan penelitian terdahulu yang relevan dengan penelitian.

BAB III METODE PENELITIAN

Bab ini menjelaskan alasan peneliti memilih penelitian kualitatif, beserta menjabarkan jenis data yang digunakan, rancangan dan tahapan penelitian, objek penelitian, , instrument penelitian, teknik pengumpulan data, hingga teknik analisis data.

BAB IV ANALISIS DATA DAN PEMBAHASAN

Bab ini menjelaskan hasil analisis dari data yang sudah diperoleh, kemudian hasil analisis tersebut disusun dengan cara sistematis untuk menjawab rumusan masalah.

BAB V PENUTUP

Bab ini memberikan kesimpulan atas hasil analisis yang diperoleh dari bab sebelumnya, kemudian bab ini juga

menjelaskan implikasi penelitian, dan saran untuk penelitian selanjutnya.

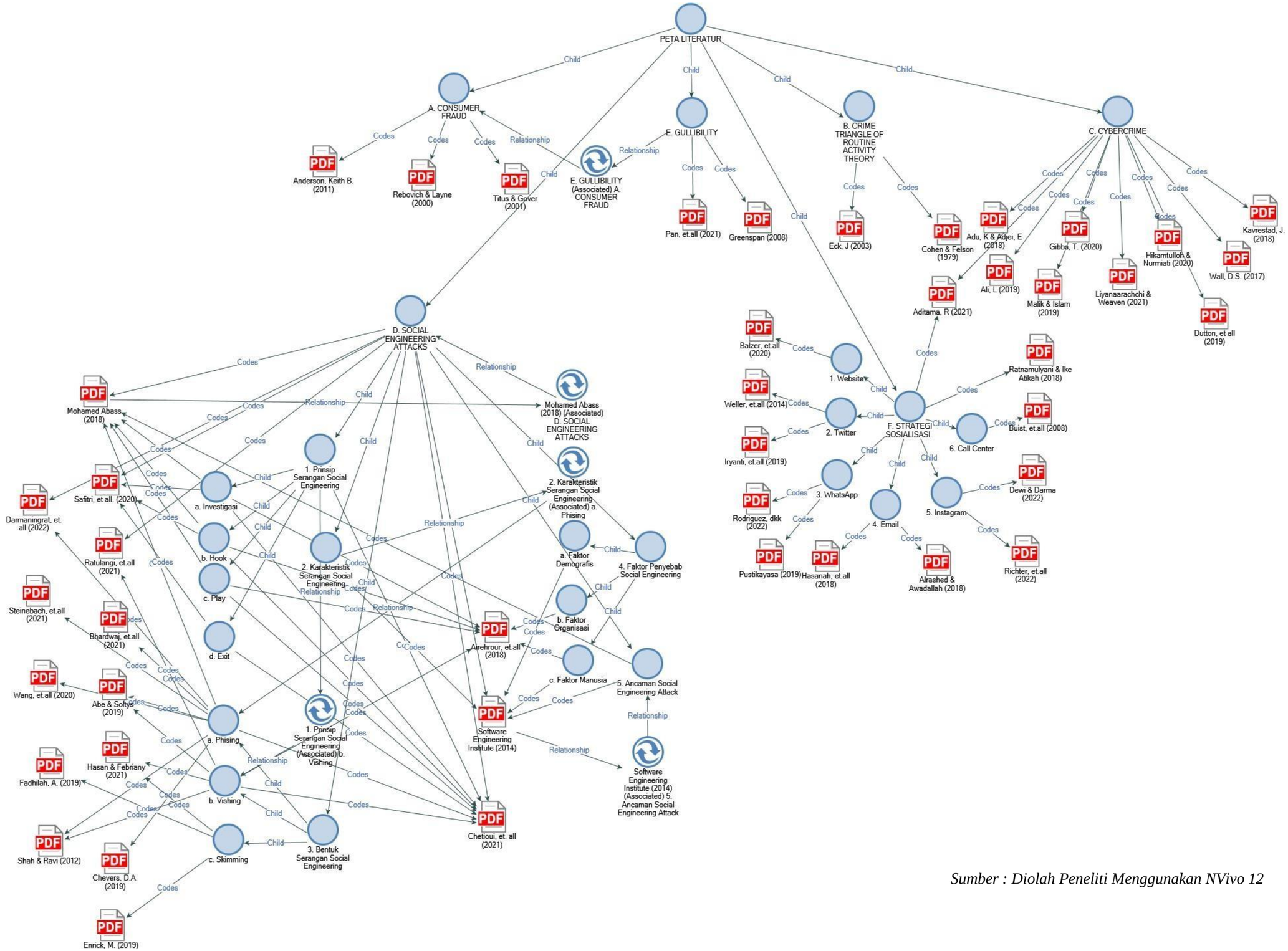
BAB II

KAJIAN PUSTAKA

2.1 Pengenalan Bab

Pada bab ini akan menjelaskan beberapa kajian pustaka yang digunakan sebagai acuan berfikir dan menganalisis. Sumber yang digunakan dalam kajian pustaka berasal dari undang – undang, artikel jurnal, perarturan , situs resmi, media online, buku, serta hasil penelitian terdahulu. Secara umum kajian pustaka pada penelitian ini akan menguraikan teori dan konsep tentang penipuan *social engineering* di sektor perbankan. Selanjutnya kajian pustaka tersebut di visualisasikan dalam bentuk peta literatur penelitian yang terdapat dalam gambar II.1 :

Gambar II. 1 Peta Literatur Penelitian



Sumber : Diolah Peneliti Menggunakan NVivo 12

2.3 Consumer Fraud

Consumer Fraud umumnya didefinisikan sebagai praktik bisnis menipu yang dapat menyebabkan konsumen mengalami kerugian finansial atau kerugian lainnya. Para korban percaya bahwa mereka ikut berpartipasi dalam transaksi bisnis yang sah, namun sebetulnya transaksi tersebut adalah penipuan. Menurut Titus, R. M. & Gover (2001) dalam penelitian nya bahwa korban menjadi "fasilitas" dalam penipuan ini. Adapun jenis penipuan yang melibatkan beberapa unsur kerjasama dengan korban diantaranya:

1. Korban melakukan kontak awal dengan pelaku atau mengambil langkah – langkah yang mengarahkan ke kontak awal (misalnya, dengan mengirimkan kupon sebagai tanggapan atas iklan "liburan gratis," atau dengan mengunjungi situs web yang menjanjikan pengembalian investasi yang luar biasa,
2. Korban memberikan informasi pribadi dirinya yang membantu pelaku melakukan penipuan,
3. Korban membiarkan pelaku mengubah apa yang seharusnya menjadi hubungan bisnis dan menjadi hubungan pribadi untuk menciptakan rasa percaya dan untuk mendapatkan pengabaian dari perlindungan adat.
4. Korban membiarkan pelaku membuat skenario atau versi kejadian, dan pelaku yang mengatur arena penipuan
5. Korban memberikan akses dana dengan menulis cek dan memberikan kartu kredit atau nomer rekening bank,

Adapun jenis penipuan *consumer fraud* yang sering terjadi diantaranya penipuan produk, promosi hadiah palsu, ditagih untuk membeli walaupun dalam

posisi tidak setuju, ditagih pembelian layanan internet yang tidak disetujui pembelian nya, dan penipuan program kerja di rumah (Anderson, 2011).

Selain itu, dalam penelitian Rebovich & Layne (2000) mengembangkan indeks "risiko" terhadap perilaku yang dianggap mengekspos konsumen kepada penipuan. Penelitian ini yang menyebutkan terdapat beberapa faktor yang membuat korban rentan terhadap kejahatan kerah putih *(white collar crime),* yaitu

1. Pernah menanggapi pesan yang tidak diminta, dengan membeli barang untuk memenangkan hadiah gratis,
2. Pernah memberikan PIN atau kode ATM kepada orang lain,
3. Diabaikan untuk melakukan pemeriksaan latar belakang pada kontraktor,
4. Diabaikan untuk menghancurkan permintaan kartu kredit,
5. Memberikan nomor kartu kredit korban melalui telepon nirkabel,
6. Mengalami kesulitan dalam menolak promosi penjualan.

2.4 Crime Triangle of Routine Activity Theory

The crime triangle atau segitiga kejahatan merupakan teori kriminologi lingkungan yang sering disebut *Routine Activity Theory* (RAT). Teori ini pertama kali diciptakan oleh Marcus Felson dan Lawrence Cohen pada tahun 1979. Pada umumnya *Routine Activity Theory* memberikan analisa yang berkaitan dengan faktor – faktor pendukung terjadinya kejahatan. Menurut Cohen & Felson (1979) setidaknya terdapat tiga element dimana peristiwa kejahatan itu terjadi yaitu

1. Pelaku yang termotivasi, yaitu seseorang yang mampu, mau, dan cenderung melakukan kejahatan.

2. Korban atau target yang cocok, yaitu orang atau suatu hal yang membuat pelaku untuk memenuhi tujuan kriminal.
3. Tidak adanya penjaga *(guardian),* yang mampu untuk mencegah kejahatan.

Ketiga elemen diatas harus menyatu dalam konteks tempat / waktu atau pengaturan spasial. Tidak akan muncul indikasi peluang tanpa pelaku termotivasi berkumpul di tempat dan waktu yang bersamaan dengan korban atau target yang sesuai dan tanpa didampingi penjagaan yang mampu mencegah kejahatan. Dalam teori ini poin utama nya adalah menekankan pada aktivitas rutin korban yang telah diketahui oleh pelaku yang akan meningkatkan kesempatan terjadinya kejahatan. Kegitan rutin dapat terjadi di rumah, dalam pekerjaan jauh dari rumah, dan kegiatan lain di luar rumah (Cohen & Felson, 1979).

Teori ini menunjukkan perkembangan yang signifikan dengan perluasan penerapan yang menjelaskan perubahan tingkat kejahatan dari waktu ke waktu, yang nanti nya diperlukan untuk acara pidana dan menjadi unsur pencegahan, serta memberikan konsep mengenai masalah kejahatan dalam hal elemen – elemen yang diperlukan. Zaman sekarang ini kejahatan semakin besar, tidak mengenal batasan ruang, dan telah mengglobal, sehingga perspektif yang perlu digunakan untuk melihat kejahatan harus adaptif. Begitu pula dengan *routine activity theory* yang dicetuskan oleh Cohen dan Felson yang mulai dikembangkan beberapa decade yang lalu.

Gambar II. 2 Crime Triangel of Routine Activity Theory

Sumber : Eck (2003)

Menurut Eck (2003) segitiga kejahatan yang terdapat pada gambar II.1 menerangkan bahwa terdapat perubahan element dari segitigas versi asli, segitiga yang terdapat bagian dalam merupakan segitiga kejahatan yang versi asli yaitu terdapat tiga elemen *target, offender,* dan *place.* Sedangkan untuk versi terbaru nya terdapat segitiga di lapisan luar nya yaitu *guardian, handler, manager* yang hal ini berfungsi sebagai *controllers* dari setiap elemen segitiga kejahatan yang berada di lapisan dalam. Posisi *controllers* memiliki peran penting dalam mencegah terjadinya kejahatan serta memiliki tanggung jawab terhadap elemen – elemen yang ada di lapisan bagian dalam segitiga kejahatan *(crimes triangle).* Keberadaan *controllers* di *crime triangle* mampu membuat pelaku tidak dapat bertindak. Kejahatan muncul ketika *offenders* dan *targets* bertemu berulang kali dan *controllers* gagal mencegahnya.

Pada konteksnya teori *crime triangle* berhubungan dengan penelitian ini mengenai "Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter". Pada penelitian ini, keberadaan

controllers diibaratkan sebagai pihak bank yang memiliki peran penting untuk mengatasi suatau masalah yang dialami oleh nasabah bank yang menjadi korban penipuan. Adapun penjelasan elemen – elemen yang berada diluar segitiga kejahatan *(crime triangle),* yaitu

1. *Handler*, pelaku yang telah dikenal oleh orang – orang sekitar seperti orang tua, saudara, teman, dan majikan yang memungkinkan untuk memantau atau mengendalikan tindakan pelaku.
2. *Guardian*, perlindungan dalam hal ini dapat berasal dari orang tua, saudara, petugas polisi, atau CCTV sebagai alat perlindungan secara tidak langsung yang dapat melindungi korban/target.
3. *Manager*, seseorang yang memiliki tanggung jawab pada tempat tersebut seperti manager toko atau karyawan.

Oleh karena ini itu *Routine Activity Theory* lebih konkrit jika digunakan untuk menjelaskan kasus penipuan di sektor perbankan seperti *phising, vishing,* dan *skimming.* Maka berdasarkan teori *crime triangle,* peneliti beranggapan bahwa faktor pengamanan yang lemah merupakan salah satu faktor pendukung dari kejahatan di sektor perbankan ini. Dengan demikian, jika dianalisa kejahatan seperti *phising, vishing, skimming,* dan lain – lain menjadi relevan dengan *routine activity theory.*

2.5 Cybercrime

Kävrestad (2018) mendefinisikan *cyber crimes* merupakan kejahatan yang menggunakan komputer untuk melakukan kejahatan di komputer lain. Selain itu Kävrestad (2018) juga menuturkan *cyber crime* dapat dilakukan oleh seseorang

yang memiliki pengetahuan tentang komputer. Menurut Hikmatulloh dan Nurmiati (2020) mendefinisikan *cyber crime* adalah sebuah perbuatan illegal yang menggunakan computer sebagai perantaranya, dan dapat digunakan melalui jaringan elektronik global.

Dewasa ini kebutuhan jaringan internet banyak digunakan dari berbagai kalangan, dan tentunya hal ini dapat mengakibatkan penggunaan komputer dan *smartphone* juga meningkat. Hal ini menandakan bahwa penggunaan teknologi yang semakin tinggi karena memiliki berbagai manfaat yang dapat membantu aktivitas sehari – hari. Namun dibalik sejuta manfaat nya terdapat dampak negatif, yaitu adanya pelaku *fraud* yang memanfaatkan teknologi sebagai alat melakukan kejahatan siber untuk kepentingan pribadi yang dapat merugikan orang lain.

Wall (2017) mengatakan dengan adanya perkembangan teknologi, justru dapat menciptakan kejahatan siber. Lebih lanjut Gibbs (2020) menuturkan bahwa pertumbuhan konektivitas komputer secara eksponensial dapat memperluas jenis dan jumlah peluang *cyber crimes*. Aditama (2021) menjelaskan umumnya *cyber crime* mengacu pada perangkat komputer dan alat – alat teknologi yang terhubung dengan jaringan internet. Adapun tindakan *cyber crime* menurut M. S. Malik dan Islam (2019) adalah mengakses data rahasia pengguna tanpa izin, serangan pada DOS, penyebaran virus, penipuan secara online dan komunikasi salah arah, pencurian *property*, gangguan atau intervensi sistem, pencucian uang dan peretasan.

Jadi dapat dikatakan bahwa serangan siber merupakan kejahatan yang menggunakan computer sebagai alat bantu, objek, ataupun sarana yang tindakan

tersebut dapat merugikan pihak lain demi menggapai keuntungan pribadi. Tindakan kejahatan siber tidak terlepas dari tiga hal yaitu muncul karena adanya sarana, motif, dan peluang. Menurut Kävrestad (2018) *cyber crime* terbentuk karena adanya sarana dan peluang yang kemudian akan melibatkan alat dan pengetahuan yang sudah terkomputerisasi. Maka dari itu diperlukan pengamanan sistem informasi pada jaringan internet, karena jaringan internet yang sangat rentan terhadap berbagai kejahatan. Hal ini terjadi karena internet mudah diakses secara publik sehingga memungkinkan terbuka peluang untuk melakukan tindakan penipuan (*fraud*).

Perkembangan teknologi yang semakin pesat dan meningkatnya pengguna internet membuat *cyber crime* menjadi wadah bagi *frauder* untuk mencari keuntungan dan mendapatkan kekayaan secara instan. Wall (2017) mengatakan dengan adanya teknologi digital dan jaringan internet yang lebih canggih membuat kejahatan siber lebih otomatis. Terlebih lagi di sektor perbankan banyak mengatur masalah keuangan yang aktivitas nya menggunakan teknologi modern dan jaringan internet, sehingga sector perbankan menjadi sasaran empuk bagi *frauder*.

Tindakan *cyber crime* dapat dilakukan dari mana saja karena tindakan kejahatan nya melalui internet sehingga dapat diakses tanpa batasan jarak maupun waktu yang dapat membuka peluang bagi *frauder*. Wall (2017) mengatakan bahwa faktanya sekarang tindakan *cyber crime* dapat dikendalikan hanya dengan satu atau dua orang saja dengan di dampingi keahlian khusus dan pemahaman yang mendalam mengenai *cyber crime*. Dutton et al. (2019) menjelaskan sudah menjadi bentuk keamanan bagi pengguna internet, ketika internet sudah di desain untuk

dapat mengakses yang lebih besar di berbagai tingkatan komputasi dan jaringan komunikasi. Oleh karena itu, penting bagi nasabah untuk mengetahui teknik dan metode yang digunakan oleh *fraudsters* (Ali, 2019).

Adu dan Adjei (2018) menjelaskan bahwa sisi dari *cyber crime* dapat menimbulkan salah satu resiko terbesar bagi data perusahaan yaitu kehilangan data privasi nasabah karena disebabkan kelalaian karyawan dalam pengelolaan data nasabah pada drive USB. Maka sudah menjadi tanggung jawab bagi perusahaan perbankan untuk memberikan perlindungan kepada nasabah dengan memberikan langkah – langkah proaktif agar dapat menjaga kualitas layanan perbankan. Liyanaarachchi et al. (2021) mengatakan bahwa kegagalan atau keberhasilan dalam online perbankan ditunjukkan dari penilaian konsumen terhadap kualitas dan efisiensi layanan secara online, penjualan dan pemasaran, serta penggunaan layanan lewat situs web. Selanjutnya Liyanaarachchi et al. menjelaskan bahwa perusahaan yang ingin meningkatkan penjualan dan loyalitas nasabah dalam waktu jangka panjang dapat melakukan dengan cara meningkatkan kepercayaan dan reputasi perusahaan.

2.6 *Social Engineering Attacks*

Dunia sudah melekat dengan penggunaan internet, sehingga membuka peluang bagi organisasi khususnya di sektor perbankan untuk memberikan layanan kepada nasabah nya. Transaksi dalam skala kecil hingga operasi perusahaan dapat dilakukan dengan instan karena hadirnya internet. Namun, dengan kemudahan operasi perbankan terdapat beberapa ancaman dan kerentanan keamanan privasi.

Terdapat banyak kasus, jaringan internet digunakan untuk mencuri informasi pribadi seperti kejahatan *phising*, sehingga diperlukan kewaspadaan untuk melindungi diri dari serangan tersebut. Penyerang dapat dengan mudah menggunakan informasi yang terdapat dalam akun jejaring sosial seperti facebook, *email*, instagram, twitter, whatsapps untuk membantu mencuri identitas seseorang. Maka dari itu, diperlukan tindakan pencegahan yang dapat membantu mengurangi serangan tersebut yaitu serangan *social engineering*.

Ratulangi et al., (2021) mendefinisikan *social engineering* sebagai manipulasi psikologis seseorang yang bertujuan mendapatkan informasi tertentu dengan cara menipu secara halus, secara sadar atau tidak dengan melalui telepon atau berbicara secara langsung. *Social engineering* sering digunakan oleh penyerang untuk mendapatkan informasi yang penting karena penyerang memahami bahwa manusia atau user merupakan mata rantai terlemah walaupun programmer telah membangun sistem keamanan yang baik (Safitri et al., 2020).

Definisi *social engineering* menurut Chetioui et al., (2022) yaitu seni dalam mempengaruhi suatu invidu untuk mendapatkan informasi rahasia seperti kata sandi, alamat, informasi detail yang berkaitan dengan bank. Software Engineering Institute (2014) mendefinisikan *social engineering* dalam konteks keamanaan informasi yaitu memanipulasi seseorang secara tidak sadar untuk melakukan tindakan yang dapat merugikan terhadap kerahasiaan, integritas, atau ketersediaan sumber daya atau asset organisasi, termasuk informasi, sistem informasi, atau sistem keuangan. S*ocial engineering* merupakan salah satu teknik *hacking* yang paling mudah di lakukan dengan mengeksploitasi kelemahan manusia seperti rasa

takut, rasa percaya, dan rasa ingin tolong menolong (Tyas Darmaningrat et al., 2022).

Serangan *social engineering* termasuk serangan yang berbahaya dan perlu diwaspadai guna menjaga keamanan informasi. *Social engineering* merupakan serangan psikologis yang menyerang manusia dengan cara menipu untuk sesuatu yang seharusnya tidak dilakukan. Menurut Abass (2018) manusia sangat mudah dimanipulasi untuk dapat memberikan informasi atau detail lainnya yang berguna bagi penyerang. Selain itu manusia juga lebih mudah untuk diretas daripada sistem dan jaringan komputer (Abass, 2018).

Manusia yang memiliki sifat ceroboh, malas, dan memiliki antusiasme yang tinggi dapat dimanfaatkan penyerang sebagai target. Berawal dari sinilah keahlian *social engineering* sangat diperlukan, karena inti dari pembahasan *social engineering* adalah menemukan kelemahan manusia yang nantinya akan dimanfaatkan *hacker* untuk menemukan informasi yang penting. Walaupun sistem komputer telah diberikan pengamanan dan lindungi dengan piranti keras dan lunak yang canggih, yang memungkinkan dapat menangkal serangan seperti firewalls, anti virus, dan lainnya. Namun, jika manusia yang lalai dalam mengoperasikan nya, maka peralatan tersebut tidak dapat berguna sepenuhnya.

Hadirnya teknologi membuat penyerangan lebih efektif seperti korban tidak dapat melihat pelaku secara fisik, pelaku dapat berpura – pura menjadi siapa pun untuk menglabui korban yang seolah – olah pelaku merupakan orang yang terpercaya atau berasal dari lembaga resmi. Banyak kekeliruan yang dipahami oleh orang banyak bahwa pada umumnya pelaku penyerangan menggunakan alat dan

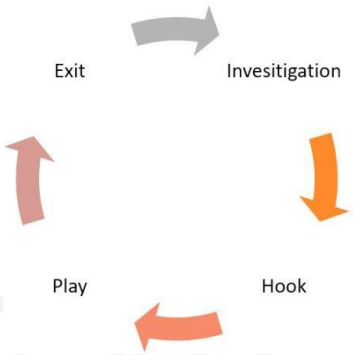
teknik sebagai alat bantu untuk meretas ke komputer atau akun korban. Namun yang sebenarnya adalah pelaku penyerangan telah memahami cara yang mudah dan lebih efektif dalam mencuri informasi pribadi korban yaitu menipu korban agar melakukan kesalahan.

Pada umumnya *social engineering* terbagi dua jenis yaitu berbasis interaksi komputer dan berbasis interaksi sosial. Abass (2018) mengatakan so*cial engineering* berbasis komputer yaitu pendekatan yang menipu korban nya agar percaya bahwa korban sedang berinteraksi dengan sistem komputer yang sebenarnya, sehingga membuat korban memberikan informasi rahasia. Sedangkan *social engineering* berbasis interaksi sosial merupakan penipuan yang mengambil keuntungan dari ketidaktahuan korban, dan memanfaatkan kecenderungan alami manusia untuk membantu dan disukai.

2.6.1 Prinsip Serangan *Social Engineering*

Serangan *social engineering* merupakan serangan yang difokuskan pada cara orang berfikir, merespon, dan berperilaku. Penyerang terlebih dahulu harus mengetahui cara yang dapat mempengaruhi korban agar dapat mengikuti perintahnya, sehingga dari langkah tersebut penyerang dapat dengan mudah untuk melalukan serangan. Sebagian besar serangan *social engineering* mengandalkan proses komunikasi secara langsung antara penyerang dengan korban. Pada proses komunikasi tersebut, penyerang akan melakukan berbagai cara untuk meyakinkan korban. Keberhasilan dari serangan *social engineering* tentunya memiliki langkah yang tepat bagi penyerang untuk melakukan aksinya. Terdapat empat langkah dalam siklus *social engineering* :

Gambar II. 3 Siklus Hidup *Social Engineering*



Sumber : Chetioui et al. (2022)

1. Investigasi

Chetioui et al. (2022) mengatakan dalam langkah ini penyerang memilih korban yang dituju, kemudian melakukan penggalian informasi atas latar belakang kehidupan korban, dan selanjutnya menentukan metode serangan yang akan dipakai. Pesatnya pertumbuhan teknologi, membuat penyerang *social engineering* mudah untuk mencari informasi melalui jaringan sosial, seperti facebook, twitter, dan jaringan lainnya. Menurut Abass (2018) jenis informasi yang dicari seperti informasi pribadi, foto, lokasi, teman, bisnis, serta hal yang disukai dan tidak disukai. Airehrour et al. (2018) mengatakan hasil akhir penyerangan tergantung dari kualitas informasi yang telah dikumpulkan dari tahap ini, yang kemudian data tersebut digunakan untuk mensukseskan serangan. Tujuan pelaku pada tahap ini yaitu mempelajari informasi yang di dapatkan agar pelaku dapat menyamar menjadi pegawai, kontraktor atau vendor (Safitri et al., 2020).

2. *Hook*

Chetioui et al. (2022) mengatakan bahwa dalam langkah ini penyerang melakukan pendekatan dengan korban, dan mencoba menjalin hubungan lebih dekat untuk mendapatkan kepercayaan. Pendekatan dengan korban dilakukan untuk membangun kepercayaan kepada korban dengan mengaku bahwa penyerang merupakan anggota lembaga yang lebih senior (Abass, 2018).

Safitri et al. (2020) mengatakan dalam tahap ini, pelaku akan mengidentifikasi mata rantai yang terlemah, umumnya target nya adalah *help desk*, resepsionis, dan asisten administrasi karena bagian – bagian tersebut banyak mengetahui informasi penting. Terkadang, ketika korban diberitahu bahwa penyerang merupakan orang tertentu, umumnya korban menerima pernyataan itu dan tidak mengelak. Adapun teknik *social engineering* yang digunakan dalam tahap ini untuk memastikan korban percaya dengan penyerang yaitu mengumpulkan data seperti nama publik, informasi detail karyawan dan perusahaan (Airehrour et al., 2018).

3. *Play*

Setelah penyerang menjalin hubungan yang lebih dekat dengan korban, langkah selanjutnya menurut Chetioui et al. (2022) adalah penyerang mulai melakukan tindakan untuk memanipulasi korban dan kemudian mendapatkan informasi yang diperlukan. Menurut Abass (2018) dalam langkah ini penyerang menggunakan teknik manipulasi untuk mendapatkan target dalam keadaan emosional, sehingga penyerang harus mempelajari keadaan emosi korban nya untuk menggunakan keuntungan tersebut. Pada tahap ini penyerang memanipulasi dan mengeksploitasi kerpercayaan dan mencuri informasi secara diam – diam seperti *email spoof, scam phone calls*, atau instalasi malware (Airehrour et al., 2018).

4. *Exit*

Kemudian tahap selanjutnya adalah *exit*. Safitri et al. (2020) mengatakan tahap exit ini merupakan tahap menyelesaikan interaksi dengan korban. Pada tahap *exit* ini, penyerang telah menerima informasi yang diperlukan atau korban telah melakukan perintah yang diinginkannya, kemudian penyerang akan mengakhiri komunikasi dengan korban dan beralih ke target yang baru (Chetioui et al., 2022).

2.6.2 Karakateristik Serangan *Social Engineering*

Serangan s*ocial engineering* saat ini telah menjadi ancaman keamaan yang berbahaya bagi sebuah organisasi atau individu. Kemampuan penyerangan dalam memanipulasi korban menjadi indikator tingkat keberhasilan dari teknik *social engineering* yang digunakan oleh penyerang. Keberhasilan dari serangan *social engineering* dapat dilihat dari penyerang akan mendapatkan akses yang sah untuk melihat informasi rahasia.

Serangan *social engineering* tentunya memiliki karakteristik yang menonjol, sehingga perlunya mengetahui karakteristik tersebut sebagai langkah preventif untuk menghindari serangan *social engineering*. Software Engineering Institute (2014) merangkum beberapa karakteristik serangan *social engineering*, sebagai berikut *:*

Tabel II. 1 Rangkuman Karakteristik Serangan *Social Engineering*

Karakteristik Yang Menonjol	Informasi Umum Yang Sering Diminta
Seruan 1. Umumnya kabar baik atau buruk 2. Keterdesakan	1. Informasi akun 2. Nama belakang 3. Kata sandi dan PIN

3. Masalah sensitive atau sifatnya rahasia Respon Yang Diinginkan 1. Memberikan informasi yang spesifik 2. Memperbarui informasi pribadi/akun 3. Mengklik tautan di pesan email 4. Membuka lampiran yang dikirimkan Indikator Yang Mencurigakan 1. Memberikan salam secara umum 2. Kontek yang mencurigakan 3. Tata Bahasa atau ejaan yang buruk 4. Pengirim yang aneh atau tidak biasa 5. Informasi yang salah 6. URL yang disematkan tidak sah	4. Nomor kartu kredit 5. Nomor KTP 6. Nomor rekening bank 7. Kode bank yang digunakan 8. Alamat email 9. Nomor telepon 10. Dan informasi pribadi lainnya

2.6.3 Bentuk Serangan *Social Engineering*

1. Phising

Teknik serangan *phising* merupakan serangan yang populer di dunia perbankan. Wang et al. (2020) mengatakan bahwa serangan *phising* terjadi pertama pada tahun 1996 yang dirancang untuk mencuri nama pengguna, kata sandi, nomor kartu kredit, dan informasi pribadi lainnya. Definisi *phising* menurut Chetioui et al. (2022) merupakan bentuk di menyesatkan. Serangan *phising* disebut juga sebagai

teknik penipuan yang bertujuan untuk mendapatkan informasi pribadi (Abass, 2018).

Steinebach et al. (2021) mengatakan bahwa penyerangan *phising* dilakukan dengan meniru identitas pihak terpercaya oleh *frauder* untuk mencuri uang, informasi dan lainnya. Lebih lanjut Shah dan Ravi (2012) mengatakan penyerangan ini dapat melalui *email*, sms, *internet protocol*, dan situs web.Teknik serangan ini, penyerang akan berpura – pura menjadi organisasi atau individu terpercaya yang memaksa korban nya untuk mengungkapkan informasi pribadi. Umumnya penyerangan ini dilakukan dengan mengirimkan *email* yang menyamar bahwa *email* yang dikirim ke nasabah berasal dari bank asli (Chevers, 2019).

Bhardwaj et al. (2021) mengatakan serangan *phising* ini yang diperlukan adalah informasi pribadi yang detail, dengan cara menggunakan *email* dan web links yang tentunya dengan cara yang jahat. Setelah itu *frauder* akan membuat situs web yang seolah – olah mirip dan terkesan asli milik perusahaan perbankan dan kemudian mendorong calon korban untuk masuk ke situs tersebut dengan memerintahkan untuk mengisi informasi sensitive. Contohnya yaitu *email* yang dikirimkan kepada korban yang memberi tahu tentang pelanggaran kebijakan yang membutuhkan tindakan segera, seperti diperlukan perubahan kata sandi. Tindakan ini nantinya akan masuk pada tautan ke situs website yang tidak sah, walaupun penampilan nya hampir sama dengan versi yang sah, sehingga mendorong korban untuk tidak curiga yang kemudian korban akan memasukan kredensial dan kata sandi baru (Tyas Darmaningrat et al., 2022).

Jadi *phising* merupakan cara *frauder* untuk mendapatkan informasi yang bersifat rahasia seperti *username, password*, dan infromasi lain nya yang terkait dengan kartu kredit yang menyamar sebagai perusahaan terpercaya melalui komunikasi eletronik. Teknik *phising* ini dirancang dengan membuat link yang terdapat dalam pesan *email* yang link tersebut berisi situs web palsu yang dimiliki oleh perusahaan tipuan.

2. Vishing

Vishing atau Voice phising merupakan jenis penipuan dari *phising*, sama halnya dengan *phising* bahwa teknik penipuan nya dengan cara mengatasnamakan pihak terpercaya agar dapat menglabui nasabah. Namun teknik yang dilakukan pada *vishing* adalah penipuan kepada nasabah melalui telepon, yang suara penipu ketika bicara seolah – olah mirip dengan petugas bank.

Pengertian *vishing* menurut Hasan dan Febriany (2021) yaitu *frauder* yang melakukan penipuan nya dengan cara pendekatan terhadap korban untuk memperoleh informasi atau mempengaruhi korban melalui telepon. Airehrour et al. (2018) mendefinisikan *vishing* sebagai serangan yang menggunakan panggilan telepon untuk menipu korban nya, agar korban nya dapat mengungkapkan informasi sensitif seperti nomor kartu kredit, kode pin atau alamat rumah secara detail. Selain itu, *vishing* merupakan sebuah tindakan criminal yang menggunakan *voice email, voice over internet* (VoIP), telepon rumah atau seluler untuk mengakses informasi pribadi dan keuangan dari nasabah agar dapat melakukan pencurian indetitas yang bertujuan mendapatkan imbalan *financial* (Shah & Ravi, 2012).

Chetioui et al. (2022) mengatakan teknik *vishing* menggunakan ide yang sama dengan teknik *phising.* Menurut Ratulangi et al. (2021) *vishin*g merupakan upaya penipu dalam melakukan pendekatan terhadap korban untuk mendapatkan informasi atau mempengaruhi korban untuk melakukan tindakan dan biasanya melalui telepon. Chetioui et al. (2022) memberi contoh yang lain mengenai *vishing* yaitu penipu akan mengirim *email* ke korban yang mengaku seolah – olah dari bank, yang kemudian meminta korban untuk menghubungi nomor telepon bank yang tercantum di *email* untuk mengkonfirmasi identitas korban dengan memasukkan kata sandi. Panggilan telepon yang meminta informasi pribadi seperti ini tidak hanya menyerang aktivitas bisnis, namun dapat menyerang secara efektif terhadap nomor telepon pribadi (Abe & Soltys, 2019).

3. Skimming

Pengertian *skimming* menurut Hasan dan Febriany (2021) adalah sebuah tindakan pencurian data nasabah yang aksinya menggunakan bantuan alat perekam data. Pada metode *skimming* ditunjukkan proses perolehan nomor pin nasabah yang dilakukan oleh *frauder* sehingga *frauder* dapat mengakses mesin ATM dengan menggunakan data nasabah. Adapun cara lain yang sering terjadi, yaitu dengan mengintip dari belakang nasabah ketika nasabah sedang melakukan transaksi di mesin ATM.

Selain itu menurut Enrick (2019) ada cara lain yaitu dengan mencuri data nasabah yang sudah tersimpan dalam *magnetic strip* yang terdapat di kartu ATM dan kemudian dikirim secara nirkabel. Langkah pertama yang dilakukan oleh *frauder* yaitu memasang alat skimmer yang terletak di mulut mesin ATM,

kemudian memasang kamera tersembunyi untuk memonitor gerakan jari nasabah. Selain memasang kamera tersembunyi, *frauder* juga memasang *wifi pocket router* saat memasukan pin ATM sehingga *frauder* dapat mengetahui data nasabah dan menyalinnya ke dalam kartu palsu (Fadhilah, 2019).

2.6.4 Faktor Penyebab *Social Engineering*

Hanya berbekal data personal korban, penyerang dapat mengendalikan dan mengontrol akun korban melalui aplikasi tanpa melewati proses verifikasi. Modus penipuan *social engineering* seperti ini, tentunya memiliki faktor penyebab sehingga serangan *social engineering* dapat terjadi. Berdasarkan penelitian Software Engineering Institute (2014) mencatat bahwa terdapat tiga faktor yang menjadi penyebab terjadinya serangan *social engineering* diantaranya :

1. Faktor Demografis

Pada faktor demografis terdapat empat unsur yang mempengaruhi terjadinya serangan *social engineering* yaitu jenis kelamin, usia, kepribadian, budaya. Serangan *social engineering* ini dapat terjadi pada pria atau wanita, muda atau tua. Berdasarkan survei yang dilakukan oleh Carnegie Mellon Universty, menyatakan bahwa wanita lebih rentan terhadap serangan dibandingkan dengan pria. Hal ini dikarenakan wanita lebih nyaman dengan penggunaan media digital, sehingga memungkinkan wanita dapat membalas iklan sampah atau penawaran yang lainnya (Software Engineering Institute, 2014).

2. Faktor Organisasi

Software Engineering Institute (2014) mengatakan faktor organisasi berkaitan dengan masalah praktik manajemen, penerapan kebijakan, lingkungan kerja, beban kerja, dan usur lainnya yang berhubungan di tempat kerja yang

mempengaruhi defisiensi kinerja. Selain itu Software Engineering Institute (2014) mengatakan bahwa faktor organisasi ini lebih sulit dan abstrak karena sering kali kegagalan yang terjadi pada aspek organisasi yang lebih luas seperti contohnya adalah komunikasi yang buruk, prosedur yang membingungkan, penggunaan sistem yang salah, sumber daya yang tidak memadai, tekanan pekerjaan, serta keamaan sistem yang buruk. Sistem manajemen yang mengalami kegagalan akan memiliki dampak negatif terhadap kepuasan karyawan, hadirnya ketidakpuasan karyawan ini akan mengakibatkan karyawan menyabotase organasasi (Airehrour et al., 2018).

3. Faktor Manusia

Emosi seorang individu faktanya dapat terlihat dari karakteristik orang tersebut, lingkungan sekitarnya, kebiasaan yang sering dilakukan. Keadaan emosi yang tidak stabil ini dapat dimanfaatkan oleh penyerang untuk melakukan aksinya. Dalam penelitian Software Engineering Institute (2014) terdapat beberapa perilaku manusia yang mempengaruhi rentan nya terjadi serangan diantaranya kurangnya perhatian, kurangnya pengetahuan dan kegagalan memori, penalaran atau penghakiman yang keliru, toleransi dan persepsi resiko yang buruk, nilai kasuala tentang kepatuhan, stress, kecemasan, dan gangguan fisik. Selain itu, dengan adanya ketidaktahuan dan kurangnya kesadaran terhadap serangan siber yang menyebabkan serangan *social engineering* dapat bertumbuh dengan cepat (Airehrour et al., 2018).

2.6.5 Ancaman *Social Engineering* Attack Bagi Nasabah

Penggunaan internet yang semakin meningkat telah menjadi fasilitas bagi penyerang untuk melakukan aksinya, sehingga internet memiliki andil dalam

serangan ini. Umumnya penyerangan ini sering dialami oleh organisasi besar seperti perbankan khususnya bank. Namun, penyerangan *social engineering* lebih dominan menyerang para nasabah bank. Pelaku penipuan *social engineering* mengetauhi sisi lemah dari nasabah, yaitu mudah dimanupulasi untuk memberikan informasi atau rincian lainnya yang mungkin berguna bagi pelaku (Abass, 2018)

Oleh karena itu, terdapat beberapa dampak bagi nasabah atas penipuan *social engineering.* Dampak penipuan ini tidak hanya merugikan perusahaan perbankan namun, merugikan nasabah. Adapun ancaman penipuan *social engineering* menurut Software Engineering Institute (2014), diantaranya :

1. Kerugian keuangan
2. Pencurian identitas
3. Informasi yang bersifat rahasia, pribadi dicuri
4. Kekayaan intelektual dicuri
5. Komputer disusupi, dan ditanamkan malware atau virus
6. Data, perangkat lunak, dan/atau perangkat keras, asset dimanipulasi atau dihancurkan
7. Organisasi atau pribadi memiliki rasa malu
8. Keuntungan politik
9. Kegagalan dalam pelayanan

2.7 Gullibility

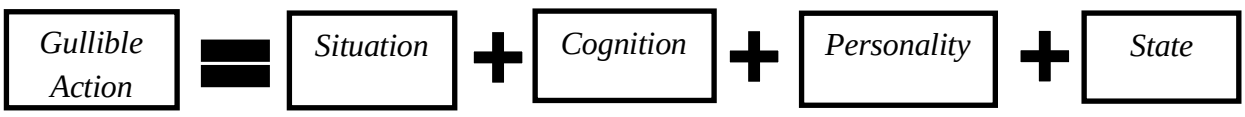
Teori ini pertama kali dibuat oleh Stephen Greenspan dalam bukunya yang berjudul *Annals of Gullibility : Why We Get Duped and How to Avoid It* yang memberikan pandangan secara komprehenisf tentang mudahnya tertipu. Menurut

Greenspan (2008) *gullibility* dapat didefinisikan sebagai kecenderungan yang tidak biasa untuk ditipu atau dimanfaatkan. Penipuan dapat terjadi pada semua kalangan. Istilah penipuan mengacu pada pola penipuan yang berulang dengan sendirinya dalam pengaturan yang berbeda, bahkan di tanda peringatan. Seseorang yang mudah tertipu melibatkan beberapa tingkat pemaksaan, khususnya dari paksaan secara psikologis (Greenspan, 2008).

Tidak heran lagi bahwa banyak orang yang mudah tertipu terhadap informasi yang salah. Pada zaman sekarang ini penggunaan internet dan media sosial sudah meningkat, sehingga bukan hal yang baru jika menemukan informasi yang salah dari sumber tersebut. Oleh karena itu, dapat dikatakan bahwa popularitas internet dan media sosial telah memfasilitasi orang untuk membagikan informasi yang salah (Pan et al., 2021).

Fenomena peristiwa penipuan perlu menjadi perhatian karena hal ini akan memberikan dampak yang negatif bagi korban baik dalam kerugian *financial*, atau pun kehidupan sosial, sehingga perlu untuk mengetahui faktor – faktor yang menjadi pemicu terjadinya penipuan sebagai upaya tindakan pencegahan penipuan. Menurut Greenspan (2008) terdapat empat faktor yang berkontribusi dalam hal mudahnya orang tertipu. Campuran dari keempat faktor ini yang menyebabkan orang mudah tertipu, yang memiliki rumus sebagai berikut :

Gambar II. 4 Rumus *Gullibility*



Sumber : Greenspan (2008)

1. Situasi, mungkin penipu sangat persuasif, atau mungkin ada orang lain yang menjamin kejujuran nya,
2. Kognisi, mungkin korban tidak dapat membaca sikap penipu atau tidak mengetahui jenis investasi yang dicakup oleh *scam*,
3. Kepribadian, mungkin korban adalah orang yang sangat dipercaya atau sulit mengatakan "tidak",
4. Keadaan, mungkin korban kelelahan atau dalam keadaan mabuk atau sangat tergantung dengan penipu.

2.8 Strategi Sosialisasi

Jaringan internet yang semakin dibutuhkan telah membuat kehidupan baru di zaman sekarang. Adanya jaringan internet memudahkan komunikasi antar individu tanpa adanya batas waktu dan jarak sehingga banyak bermunculan jenis media online sebagai media untuk berkomunikasi. Fenomena hadirnya media sosial mengubah komunikasi individu menjadi lebih mudah. Menurut Aditama (2021) media sosial merupakan media yang bersifat bebas digunakan untuk mengekspresikan dan menjelajahi pendapat yang dimiliki seseorang secara terus menerus. Media sosial dapat diartikan sebagai sarana medium berbasis teknologi internet (media online) yang memungkinkan seseorang dapat berinterkasi sosial, berkomunikasi dan bekerjasama, serta berbagi dengan orang lainnya (Ratnamulyani, Ike Atikah Maksudi, 2018).

Zaman yang sudah terhubung dengan jaringan internet, dipenuhi dengan perangkat yang saling terkoneksi. Begitu pula setiap manusia sebagai pengguna akan terkoneksi dengan jaringan. Berdasarkan data dari *Hootsuite* dan *WeAreSocial* pada bulan januari tahun 2021 ditunjukkan sebesar 5,22 miliyar pengguna unik perangkat mobile atau smarthphone, dan terdapat 4,66 miliyar pengguna internet di

seluruh dunia. Data tersebut menunjukkan bahwa lebih dari 2 per 3 manusia sudah terhubung dengan jaringan internet dan sudah menggunakan teknologi komunikasi dan informasi.

Selain itu data dari *Hootsuite* dan *WeAreSocial* menunjukkan 4,20 miliyar manusia memiliki akun media sosial yang aktif dan terkoneksi dengan keluarga, teman, kerabat, dan lain nya. Tidak hanya itu, di Indonesia sendiri menunjukkan bahwa sebesar 8 jam 52 menit penggunaan internet melalui perangkat apapun, dengan penggunaan media sosial lebih dari tiga jam. Berdasarkan data tersebut diketahui bahwa terdapat 202,6 juta pengguna internet yang 96% diantaranya merupakan pengguna *smartphone*. Hal ini menunjukkan bahwa masyarakat dengan mudah mengakses internet tak kenal tempat dan waktu. Berdasarkan data – data yang sudah dijelaskan bahwa di Indonesia penggunaan internet dan media sosial sudah melekat dengan aktivitas masyarakat di Indonesia.

Oleh karena itu, dengan hadirnya internet dapat dimanfaatkan sebagai perantara untuk menyampaikan sosialisasi pencegahan penipuan *social engineering*. Penggunaan jaringan internet membuat segala aktivitas menjadi efektif dan efisien, hal ini pun yang dapat membantu bank – bank di Indonesia untuk mesosialisasikan pencegahan penipuan. Pada penelitian ini, peneliti fokus menganalisa media website dan media sosial twitter yang digunakan sebagai media sosialisasi oleh Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI). Umumnya, sosialisasi yang diberikan melalui website dan twitter oleh bank – bank tersebut mencantumkan layanan sarana kontak yang dapat dihubungi oleh nasabah seperti whatsapp, email, Instagram, call center. Berikut ini penjelasan nya:

2.8.1 Website

Hadirnya internet membuat masyarakat ketergantungan untuk menggunakan jaringan internet karena masyarakat membutuhkan informasi, ilmu pengetahuan ataupun digunakan untuk membantu aktivitasnya agar lebih mudah. Maka dari itu, dibutuhkan aplikasi web agar dapat mempermudah dan mempercepat dalam menyampaikan informasi secara luas dan menyeluruh. Website merupakan halaman web yang berisi kumpulan informasi yang dapat menampilkan data berupa gambar, audio, video, teks dan lain nya. Selain itu website dapat diakses dengan mudah dan cepat bagi siapapun yang ingin menggunakan nya. Menurut Balzer et al. (2020) aplikasi web bertujuan untuk mengeksplorasi hubungan seluruh kumpulan data yang besar dan kompleks dengan mudah, cepat, dan interaktif.

2.8.2 Twitter

Twitter didirikan pada tahun 2006 oleh Jack Dorsey. Twitter merupakan sebuah *platform* media sosial yang mengkombinasikan media jejaring sosial dan microblog. Pada tanggal 7 November 2017 penggunaan teks yang digunakan hingga 280 karakter twit. Followers di twitter saling mengikuti akun profil, dan dapat melihat twit atau konten, walaupun tanpa perlu diikuti kembali *(follow back)* oleh akun yang di *follow*. Lewat twitter juga seseorang dapat membalas pesan atau *reply*, atau meneruskan pesan dengan format kata "retweet" atau "RT". *Sebutan trending topics* menjadi sebuah ukuran seberapa berhasilnya penyebaran informasi dalam media tersebut. Sebuah postingan berhasil menjadi *trending topic* ditunjukkan dengan banyak nya yang me-*retwit, reply*, atau *mention*. Informasi dapat tersebar secara luas dan cepat melalui twitter karena fitur retwit yang dimilikinya (Iryanti & Rahman, 2019).

Hadirnya media sosial twitter akan memudahkan organisasi dalam

membangun bisnis dan menghasilkan sentiment positif terhadap institusi. Weller et al. (2014) mengatakan twitter memiliki tiga lapisan komunikasi yaitu :

1. Lapisan Meso

Lapisan yang ditujukkan kepada pengguna yang ingin membagikan moment nya dalam sebuah twit kepada seluruh *followersnya*. Yang menunjukkan bahwa twit tersebut tidak bersifat privasi yang secara spesifik ditujukkan untuk sebuah akun.

2. Lapisan Makro

Lapisan yang menggunakan tanda pagar dalam twitnya. Tada pagar ketika digunakan dalam sebuah twit maka twit tersebut dapat dilihat oleh pengguna twitter lain walaupun tidak saling mem-*follow*. Dengan demikian, tanda pagar merupakan lapisan makro komunikasi yang luas dan menjadi perbincangan pengguna.

3. Lapisan Mikro

Dalam lapisan mikro membentuk komunikasi antar pengguna untuk melanjutkan percakapan dalam arah yang lebih sempit. Dalam lapisan ini, pengguna menyertakan *@mention* untuk menyebutkan pengguna yang lain. Maka seluruh percakapan yang dikirimkan dengan menggunakan *@mention* akan masuk kedalam kolom notifikasi pengguna lain.

2.8.3 Whatsapp

Whatsap*p* merupakan aplikasi gratis yang memberikan layanan bertukar pesan dan panggilan yang sederhana, aman, dan reliabel. Menurut Rodríguez et al. (2022) penggunaan teknologi komunikasi seperti whatsapp dapat berkontribusi sebagai fasilitator pada persepsi ketersediaan dan kedekatan profesional. Pustikayasa (2019) mengatakan penggunaan whatsapp hampir sama dengan aplikasi SMS, namun aplikasi whatsapp menggunakan jaringan internet tidak

menggunakan pulsa dan selama ponsel masih terhubung dengan layanan internet, pengguna dapat mengirim pesan melalui aplikasi whatsapp. Informasi yang dilansir dari website resmi whatsapp, terdapat beberapa fitur yang lengkap yang di sediakan oleh aplikasi whatsapp, diantaranya seperti :

1. Pengiriman pesan
2 Pengiriman foto, video dari galeri ataupun dari kamera
3 Mengirim berbagai bentuk dokumen
4 Melakukan panggilan dan mengirim pesan suara *(voice note)*
5 Membagikan lokasi dengan menggunakan GPS
6 Mengirimkan kartu kontak
7 Pengguna whatsapp dapat mengatur panel profilnya sendiri seperti nama, foto, status serta beberapa alat pengaturan privasi lainnya.

2.8.4 Email

Email merupakan singkatan dari elektronik mail atau surat elektronik dalam bentuk digital yang penggunaan nya menggunakan jaringan internet. Internet memiliki jaringan yang menguhubungkan berbagai jaringan di seluruh dunia yang memungkinkan penyampaian surat elektronis dengan cepat. Hal ini pun dikatakan juga oleh (Hasanah et al., 2018), yang mengatakan bahwa *email* merupakan salah satu layanan atau aplikasi yang sering digunakan untuk surat menyurat karena dengan keistimewaan yang di miliki *email* adalah alat komunikasi yang murah, cepet dan efisien.

Email digunakan untuk mengirimkan data seperti file teks, gambar, audio, video. Selain itu menurut (Alrashed & Awadallah, 2018) *email* juga memiliki fasilitas untuk melakukan pemindaian visual dengan cepat yang tujuan nya dapat diletakkan di sebuah folder atau dihapus. Penggunaan *email* memiliki berbagai

keuntungan bagi pengguna nya yaitu

1. Waktu lebih efisien
2. Lebih menghemat biaya
3. Penggunaan nya parktis
4. Menawarkan keamanan data
5. Dapat mensortir, menyimpan, dan menghapus data

2.8.5 Instagram

Instagram salah satu layanan jejaring sosial milik perusahaan Meta atau perusahaan induk yang juga memiliki Facebook dan Whatsapp. Instagram yang dirilis sejak tahun 2010 merupakan platform yang dominan dengan tampilan visual. Richter et al. (2022) mengatakan pengguna Instagram dapat mengedit konten foto dan video dengan menggunakan filter, dan dapat disertai dengan 2.200 karakter teks. Selain itu Richter et al. (2022) menambahkan bahwa Instagram memungkinkan pengguna dapat mengirim pesan pribadi, penggunaan *hashtag* yang berguna untuk mencari, serta membagikan *"story"*yang dapat diakses oleh orang lain untuk waktu yang terbatas. Beragamnya fungsi yang diberikan oleh aplikasi instagram dalam mengelola foto, aplikasi ini membuat ketertarikan khusus bagi pengguna instagram dan tidak hanya itu Instagram juga merupakan aplikasi untuk *photo-sharing* dan layanan jejaring sosial online yang memudahkan pengguna membagikan hasil foto lewat beragam layanan sosial media seperti Facebook, Twitter, dan situs media lain nya (Dewi & Darma, 2022).

Unggahan tersebut dapat dibagikan pada public atau dengan pengikut yang telah disetujui sebelumnya. Pengguna Instagram memudahkan pengguna menjelajahi konten yang sedang tren berdasarkan tag dan lokasi. Selain itu,

pengguna Instagram dapat menyukai atau mengomentari postingan foto atau video yang diupload oleh pengguna lain. Adapun keunggulan Instagram diantaranya :

1. Mampu menerapkan privat akun
2. Menawarkan fitur – fitur yang menarik
3. Menyediakan akun bisnis
4. Menawarkan layanan pengiriman pesan instan

2.8.6 Call Center

Buist et al. (2008) mengatakan *call center* merupakan seperangkat sumber daya untuk komunikasi antara organisasi dengan pelanggan nya melalui telepon. Secara global *call center* merupakan suatu sistem terpusat yang menerima dan mengirim permintaan panggilan yang menangani panggilan masuk dan keluar dari konsumen terkait produk atau layanan perusahaan. Layanan yang ditangani dalam *call center* seperti fitur – fitur produk, status pesanan, promosi, keluhan dan lain – lain. *Call center* umumnya diberikan oleh bank untuk memberikan pelayanan kepada nasabahnya lebih optimal. Agen *call center* sebagian besar berkomunikasi melalui telepon. Adapun tanggung jawab *call center* dalam perusahaan diantara nya

1. Memberikan informasi yang detail terkait produk atau jasa kepada pelanggan
2. Memberikan solusi atas kendala yang dialami oleh pelanggan
3. Mencatat permintaan dan keluhan nasabah yang tidak dapat diselesaikan

2.9 Penelitian Terdahulu

Penelitian Ahmadian dan Sabri (2021)yang berjudul "Teknik Penyerangan Phising Pada *Social Engineering* Menggunakan Set dan Pencegahannya" penelitian ini mengkaji cara penyerang social engineering memanfaatkan perilaku manusia dengan teknik phising dengan menggunakan SET dan dalam penelitian ini dijelaskan cara untuk mengatasi ancaman serangan *social engineering*. Pada

penelitian ini disimpulkan bahwa *social engineering* merupakan suatu teknik serangan yang mengeksploitasi kelemahan manusia. Serangan *social engineering* terbagi menjadi dua yaitu berbasis interaksi sosial, dan berbasis interaksi komputer. Serangan yang menggunakan teknik *phising* merupakan jenis *social engineering* berbasis komputer. Cara mengatasi serangan tersebut dapat dilakukan dengan password management, two-factor authentication, antivirus, change management.

Penelitian Saskara dan Arthani (2021) yang berjudul "Tinjauan Kriminologi Terhadap Kejahatan *Skimming* Melalui ATM di Polda Bali" penelitian ini mengkaji fenomena kriminalitas atas kejahatan skimming di Bali, faktor penyebab terjadinya kejahatan skimming, serta upaya penanggulangan kejahatan skimming. Hasil penelitian menunjukkan bahwa terdapat dua faktor penyebab skimming di Polda Bali yaitu faktor internal pelaku seperti kebutuhan ekonomi, faktor narkotika, dan faktor Pendidikan. Faktor eksternal dapat berasal kurangnya pengamanan, pengawasan yang ketat di mesin ATM serta lemahnya penegak hukum. Kemudian upaya penanggulan nya dapat berupa upaya pre-emtif, preventif, represif. Upaya pre-ventif seperti memberikan sosialiasi kepada masyarakat agar lebih waspada, upaya preventif yaitu bertemu dengan pimpinan lembaga perbankan yang ada di Bali agar dapat mengingatkan nasabahnya supaya berhati – hati melakukan transaksi. Selanjutnya upaya represif yaitu melakukan penangkapan dengan memberikan sanksi hukum bagi pelaku penipuan.

Penelitian Safitri et al. (2020) yang berjudul "Analisis Teknik *Social Engineering* Sebagai Ancaman Dalam Keamanan Sistem Informasi" penelitian ini menganalisa tipe penyerangan *social engineering* dan memberikan cara pencegahan serangan *social engineering*. Hasil penelitiannya menunjukkan bahwa hacker telah memiliki informasi – informasi penting yang dibutuhkan untuk menerobos sistem

keamanan, sehingga sistem keamanan menjadi tidak berguna. Teknik *social engineering* yang paling sering digunakan penyerang adalah eksploitasi internet, seperti *fake-email, phising,* dan lain sebagainya. Adapun cara pencegahan nya yaitu meningkatkan kesadaran pengguna mengenai *social engineering* dan ancamannya dengan cara mensosialisasikan agar berwaspada terhadap metode *social engineering.*

Penelitian Abass (2018) yang berjudul "*Social Engineering Threat and Defense: A Literature Survey*" penelitian ini mengkaji dampak serangan *social engineering* modern pada organisasi atau individu dan menjelaskan metode yang digunakan dalam serangan *social engineering* . Hasil penelitian nya menunjukkan bahwa manusia merupakan titik terlemah dalam sistem yang mudah untuk dimanupulasi. Meningkatnya manusia yang menggunakan sosial media, maka hal ini akan mempermudah penyerang untuk mendapatkan data pribadi dan data sensitive. Selain itu organisasi harus memiliki kebijakan untuk memberikan edukasi mengenai *social engineering* kepada pekerja dan pastikan kebijakan tersebut dijalankan untuk menghilangkan ancaman serangan *social engineering*.

Penelitian Hasan dan Febriany (2021) yang berjudul "Identifikasi Tindakan Pengawasan Dan Pencegahan Terhadap Kejahatan Finansial Perbankan Syariah Selama Masa Pandemi COVID 19" penelitian ini mengkaji tindakan yang perlu dilakukan oleh perbankan dalam pencegahan dan pengawasan yang bemanfaat selama masa pandemic COVID 19 agar tetap menjaga loyalitas kepercayaan nasabah terhadap bank. Hasil penelitian nya menunjukkan bahwa pencegahan dapat dilakukan oleh bank dengan cara preventif untuk melindungi nasabah dan karyawannya. Pencegahan dan pengawasan perlu melibatkan bank Indonesia yang memegang peran dalam pengawasan eksternal, pengawasan internal, pengawasan

masyarakat supaya dapat berjalan dengan efektif dan maksimal. Selain itu perbankan syariah dapat memberikan kebijakan kepada nasabah untuk menghindari kejahatan selama pandemic yaitu diantaranya melonggarkan fasilitas pembiayaan kepada nasabah yang terkena dampak pandemi COVID 19, memberikan berupa informasi dan edukasi kepada masyarakat melalui media massa, whatsapp, email, dan lain lain.

Penelitian Tyas Darmaningrat et al. (2022) yang berjudul "Sosialisasi Bahaya dan Upaya Pencegahan *Social Engineering* Untuk Meningkatkan Kesadaran Masyarakat Tentang Keamanan Informasi" penelitian ini membahas mengenai pemberian sosialisasi mengenai teknik *social engineering*, dampak yang ditimbulkan serta upaya pencegahan kepada masyarakat. Adapun sosialisasi yang dibagikan ke masyarakat yaitu melalui webinar di zoom, dalam webinar tersebut dibagikan pula simulasi mengenai praktik pencurian data, dibagikan poster dan video tentang teknik dan proses penipuan social engineering, poster upaya pencegahan *social engineering*, serta video pengenalan *social engineering* di youtube . Hasil penelitian nya menunjukkan bahwa sosialisasi yang diberikan melalui webinar zoom memiliki sisi positif salah satunya dapat diikuti oleh banyak masyarakat dan bisa menjangkau lingkungan yang lebih luas. Selain itu, transformasi digital yang terjadi akibat pandemi COVID-19 membuat kegiatan sosialisasi pencegahan penipuan *social engineering* yang dilakukan secara daring ini semakin relevan dengan kebutuhan masyarakat. Dengan adanya sosialisasi ini, masyarakat menjadi berpikir ulang dan lebih berhati – hati ketika membagikan informasi yang sifatnya pribadi.

Penelitian Chetioui et al. (2022) yang berjudul "*Overviwew of Social Engineering Attacks on Social Networks*" penelitian ini memberikan gambaran

mengenai prinsip, dan jenis serangan *social engineering* di jejaring sosial. Penelitian ini menunjukkan serangan *social engineering* merupakan serangan yang mudah dan otomatis dan dapat dilakukan dalam skala yang besar. Serangan *social engineering* tidak dapat dihentikan jika hanya mengandalkan sistem keamanan yang kuat. Namun, diperlukan juga untuk berinvestasi dalam hal meningkatkan kesadaran keamanan siber dengan cara mengajarkan kepada orang – orang mengenai serangan *social engineering* agar lebih sadar dan perhatian terhadap serangan tersebut.

Berdasarkan keterbatasan penelitian – penelitian yang telah dijelaskan sebelumnya, penelitian – penelitian tersebut hanya mengkaji teknik - teknik, dampak, ancaman, tindakan pencegahan dan penanggulangan dari serangan *social engineering.* Namun tidak membahas mengenai serangan *social engineering* yang sering terjadi pada nasabah bank, dan tidak mengkaji strategi pencegahan penipuan *social engineering* yang telah dilakukan oleh bank – bank sebagai upaya untuk mencegah terjadinya serangan *social engineering*. Betapa pentingnya peran bank dalam memberikan perlindungan kepada nasabah bank nya agar tidak menjadi korban akibat serangan *social engineering*. Maka dari itu, peneliti mengangkat judul penelitian mengenai "Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter". Dalam penelitian ini juga peneliti menggunakan metode *case study* dan *archival research* sebagai metode penelitian, karena dalam penelitian ini, peneliti membahas mengenai kasus - kasus *social engineering* pada nasabah bank yang pernah terjadi di Indonesia dan menganalisa pola - pola sosialisasi pencegahan penipuan *social engineering* yang telah dilakukan oleh bank – bank melalui media website dan twitter, sehingga pembahasan nya lebih komprehensif dan mendalam.

BAB III

METODE PENELITIAN

3.1 Pengenalan Bab

Bab ini akan menjelaskan metode penelitian yang digunakan selama proses penelitian yang membahas tentang Analisa Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter. Pembahasan pada bab ini penting, sebab bab ini termasuk pondasi untuk menjawab rumusan masalah yang sudah dipaparkan di bab sebelumnya sehingga pada bab ini memiliki pengaruh pada pembahasan bab selanjutnya. Selain itu, bab ini juga akan membahas tentang desain penelitian, alasan memilih penelitian kualitatif, rancangan dan tahapan penelitian, objek penelitian, instrument penelitian, sumber dan jenis data, teknik pengumpulan data, serta teknik analisis data.

3.2 Alasan Memilih Penelitian Kualitatif

Penelitian kualitatif menurut Creswell (2013) merupakan metode penelitian yang bermula dengan asumsi atau interprestasi kerangka kerja yang memahami makna masalah sosial pada individu maupun kelompok. Selain itu Saunders; Lewis; Thornhill., (2012) mengatakan bahwa penelitian kualitatif ini proses meringkas bagian data, mengkategorikan data, serta menghubungkan kategori tersebut dengan membuat struktur agar dapat menjawab rumusan masalah. Maka dari itu peneliti menggunakan metode kualitatif agar dapat mengetahui pola – pola sosialisasi pencegahan modus *social engineering* oleh bank melalui media website dan media sosial twitter.

3.3 Desain Penelitian

Berdasarkan permasalahan yang dipaparkan pada pertanyaan penelitian, maka penelitian yang tepat digunakan pada penelitian ini adalah penelitian kualitatif. Penelitian kualitatif erat hubungan nya dengan interpretasi peneliti, sehingga membutuhkan pemahaman yang dalam ketika menjelaskan mengenai "Pola – Pola Sosialisasi Pencegahan Modus *Social Engineering* Oleh Bank Melalui Media Website Dan Media Sosial Twitter".

Menurut Saunders; Lewis; Thornhill. (2012) penelitian kualitatif mempelajari makna partisipan dan hubungan diantara keduanya, yang menggunakan berbagai teknik pengumpulan, data dan prosedur analitis dalam mengembangkan kerangka konseptual. Pada penelitian kualitatif, penemuan nya bukan berasal dari proses statistik ataupun dengan proses pengukuran, namun penelitian kualitatif berfokus pada mengeksplorasi lebih dalam proses yang melatarbelakangi terjadinya fenomena tersebut

Berdasarkan rumusan masalah dan tujuan penelitian yang sudah dipaparkan di bab pertama, maka penelitian ini termasuk *multimethod qualitative* yang menggunakan metode *archival research* dan *case study*. Saunders; Lewis; Thornhill. (2012) mendifinisikan *archival research* sebagai strategi penelitian yang menggunakan catatan dan dokumen sebagai sumber utama yang dihasilkan dari aktivitas sehari – hari. Sedangkan *case study* merupakan penelitian yang dilaksanakan secara alami dengan melihat fenomena yang terjadi. Selanjutnya Saunders; Lewis; Thornhill. (2012) mengatakan bahwa *case study* digunakan dalam rangka mengeksplorasi sebuah topik penelitian atau fenomena yang berdasarkan konteks kehidupan. Penelitian yang menggunaka c*ase study* bertujuan untuk

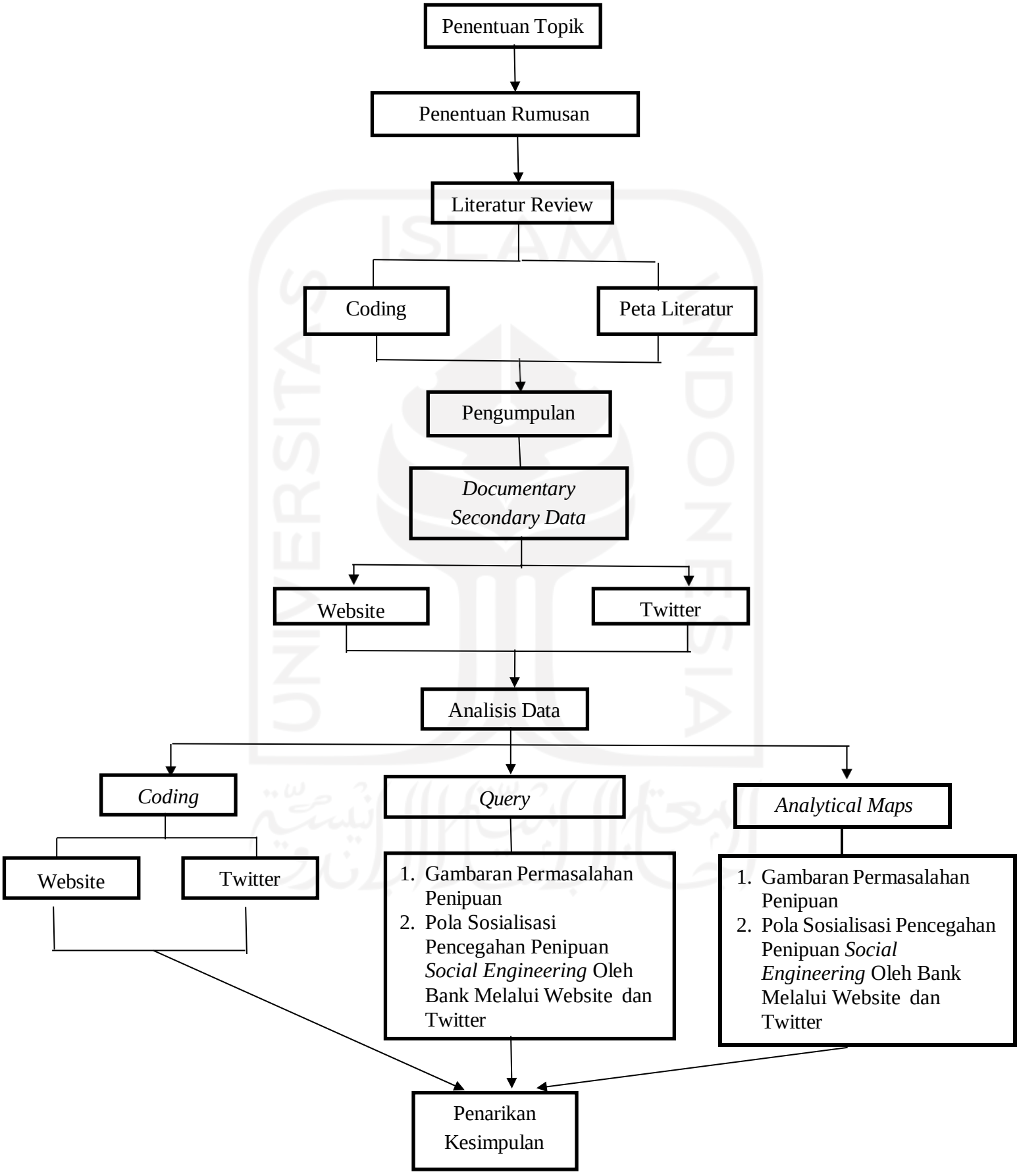
mempelajari lebih dalam mengenai keadaan kehidupan saat ini yang memiliki latar belakang interaksi dengan lingkungan suatu unit sosial (Subiyanto & Suwarto, 2007).

Penelitian ini menggunakan pendekatan induktif yang membantu untuk mengembangkan kategori menjadi sebuah kerangka atau model yang dapat membantu untuk meringkas data yang kompleks. Pendekatan induktif ini berfokus untuk menemukan konsep atau model yang di interprestasikan peneliti melalui teks yang dibaca secara detail. Berbeda hal nya dengan pendekatan deduktif untuk menguji hipotesis, asumsi, dan teori yang sudah dibuat oleh peneliti sebelumnya.

3.4 Rancangan dan Tahapan Penelitian

Rancangan penelitian dapat dimaknai dengan proses dalam mengumpulkan dan menganalisis data penelitian dengan membuat perencanaan yang diawali dengan pengamatan, analisis data, instrument penelitian yang diperlukan, sampel yang digunakan untuk menunjang hasil penelitian. Supaya penelitian berjalan dengan baik, maka diperlukan kerangka atau pondasi yang baik guna merencanakan proyek penelitian. Dengan adanya rancangan penelitian ini dapat membantu dalam proses penelitian untuk memperoleh hasil yang baik. Pada penelitian ini memiliki 6 tahapan dalam proses penelitian nya, yaitu penentuan dan pembahasan topik, penentuan rumusan masalah, review literatur, pengumpulan data, analisa data, serta langkah terakhir penarikan kesimpulan.

Gambar III. 1 Tahap Penelitian



3.4.1 Tahap Penentuan Topik Penelitian

Dalam melakukan penelitian, tahap pertama yang dilakukan oleh peneliti adalah menentukan topik yang akan dibahas dalam penelitian. Tahapan ini dilakukan oleh peneliti dengan melakukan konsultasi terlebih dahulu dengan dosen pembimbing untuk mempertimbangkan pendapat dan ide terkait topik yang akan dibahas. Selain itu, dalam mengangkat topik ini peneliti memerlukan pertimbangan supaya penulisan ilmiah ini dapat bermanfaat secara praktis dan akademis.

3.4.2 Tahap Penentuan Rumusan Masalah

Tahapan penentuan rumusan masalah merupakan hal yang utama dalam suatu penelitian, sebab berawal dari rumusan masalah akan dibahas lebih lanjut dengan proses pengumpulan data penelitian. Dalam penelitian kualitatif, rumusan masalah yang dibuat cenderung lebih dalam dan pertanyaan nya lebih spesifik, serta lebih mengutamakan kualitas daripada kuantitas (jumlah). Dengan demikian penelitian kualitatif lebih memfokuskan makna dan proses. Adapun Silverman (2013) memberikan strategi dalam membuat rumusan masalah diantara nya :

a. *Answerability* : dapat melihat data apa saja yang dibutuhkan untuk menjawabnya dan bagaimana cara data akan diperoleh
b. *Interconnectedness* : pertanyaan yang dibuat berkaitan dengan satu sama lain dalam beberapa cara yang berarti, dibandingkan tidak terhubung
c. *Substantively Relevant* : pertanyaan yang dibuat menarik dan dapat bermafaat sehinga membenarkan diperlukan adanya penelitian.

3.4.3 Tahap Pengumpulan Data

Pada tahap pengumpulan data menjelaskan bagaimana cara data yang diperlukan dapat dikumpulkan, sehingga di akhir penelitian mampu menyajikan informasi yang teruji validitasnya dan *reliable*. Dalam pengumpulan data, penelitian ini menggunakan *secondary data* yang sifatnya *documentary*. Menurut Saunders; Lewis; Thornhill., (2012) *documentary secondary data* yang jenisnya text dapat berupa buku, artikel jurnal, majalah, ataupun koran. Sedangkan *documentary secondary data* yang jenisnya *non-text* berupa rekaman suara, video, gambar, film, program televisi, DVD dan CD ROM, serta halaman wesite.

Dengan demikian dalam penelitian ini, peneliti menggunakan artikel jurnal, situs website resmi bank , serta media sosial twitter milik bank sebagai media untuk mengumpulkan data. Data diambil dengan periode waktu bulan Januari hingga Februari 2022 dengan menggunakan fitur *Ncapture* untuk men-capture konten yang terdapat di website dan media sosial twitter. Output dari *Ncapture* ini adalah data lengkap yang berkaitan dengan akun yang dicapture. *Ncapture* ini merupakan aplikasi bawaan dari Nvivo yang otomatis telah terpasang di Google Chrome. Penggunaan *Ncapture* ini mempermudah dalam memperoleh data penelitian yang berhubungan dengan analisis konten sosial media, sehingga tidak perlu lagi membaca dan menganalisis postingan satu - persatu. Langkah ini bertujuan untuk mengeksplorasi berbagai teori yang relevan dengan rumusan masalah yang sedang diteliti sebagai bahan rujukan dalam melakukan penelitian.

a. Jenis Data

Dalam penelitian ini jenis data yang digunakan adalah data sekunder. Data sekunder merupakan data penelitian yang diperoleh secara tidak langsung

yaitu dengan media perantara. Data sekunder juga dapat berupa data yang telah dikumpulkan oleh instansi terkait dan kemudian dipublikasikan secara umum kepada masyarakat. Dalam penelitian ini data sekunder yang digunakan adalah dokumentasi yang dapat diambil melalui media *website* dan media sosial twitter Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI).

b. Sumber Data

Data sekunder merupakan data yang dapat berupa tabel, catatan, sms, notulensi rapat, foto, video, rekaman audio, yang diperoleh dari dokumen –dokumen penting. Menurut Saunders; Lewis; Thornhill. (2012) data sekunder awalnya dikumpulkan untuk beberapa tujuan yang lain, data sekunder dapat dianalisis lebih lanjut untuk memberikan pengetahuan tambahan atau yang berbeda, interpertasi atau kesimpulan. Dalam penelitian ini data sekunder diperoleh dari postingan website dan media sosial twitter resmi yang dimiliki oleh Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Tabungan Negara (BTN), Bank Permata, Bank Syariah Indonesia (BSI).

3.4.4 Tahapan Analisis Data

Pada penelitian ini untuk menganalisis data, peneliti menggunakan tiga tahapan yang dikemukakan oleh Miles dan Humberman tahun 1994 yang sering digunakan oleh peneliti – peneliti kualitatif, yaitu :

a. Reduksi Data

Reduksi data merupakan proses pemilihan data, penyederhanan data, dan memberikan gambaran secara global serta singkat pada kejadian yang sedang diteliti. Menurut Saunders; Lewis; Thornhill. (2012:564) mengatakan bahwa reduksi data bagian dari proses untuk meringkas dan menyederhanakan data yang sudah dikumpulkan atau diselektif supaya dapat memfokuskan pada beberapa bagian dari data. Hal ini bertujuan untuk mengubah data dan memadatkannya. Pada penelitian ini proses analisis data menggunakan bantuan *software NVivo 12* sebagai media untuk menganalisis dan mengolah data, karena *software* ini mampu melakukan *coding* dan menampilkan diagram, tabel, grafik serta model lainnya yang diperlukan dalam penelitian kualitatif. Berikut penjelasan teknik reduksi yang digunakan dalam penelitian ini yaitu *coding*.

1. Coding

Dalam penelitian kualitatif *coding* membantu dalam menguji data mentah dengan memberi label kedalam bentuk kata – kata, frase atau kalimat sehingga memudahkan peneliti dalam membuat keputusan berdasarkan data yang dimiliki. Menurut Silverman (2013) *coding* merupakan proses menempatkan data ke dalam kategori yang ditentukan secara teoritis untuk menganalisisnya. Selanjutnya Creswell (2013) menjelaskan *coding* sebuah proses menggabungkan teks atau data visual ke dalam kategori kecil dari informasi, mencari bukti untuk kode dari database berbeda yang digunakan dalam penelitian, dan kemudian memberi label pada kode tersebut. *Coding* juga dapat diartikan sebagai proses aktif dalam mengidentifikasi, memberi label, dan mensistematisasikan data sebagai milik atau mewakili beberapa jenis fenomena (Tracy, 2013).

Dalam buku Creswell (2013) terdapat tiga fase pengkodean, diantara nya :

a) Open coding

Pada fase pertama peneliti memulai dengan fase *open coding*. Creswell (2013) mengatakan pada tahap *open coding* peneliti melakukan pemeriksaan pada teks misalnya transkrip, catatan lapangan, dokumen untuk kategori informasi yang menonjol dengan disertai teks. *Open coding* merupakan langkah pertama dalam proses analisis data dalam *grounded theory*. Saunders; Lewis; Thornhill. (2012) menambahkan bahwa penekanan dalam metode *grounded theory* yaitu untuk memperoleh makna dari subjek dan setting yang sedang di pelajari.

Metode *grounded theory* ini akan mengarahkan peneliti dalam melakukan analisis awal dengan melihat pada unit data yang lebih kecil dari pada unit yang lebih besar. Dengan demikian penelitian akan lebih mudah dikelola dan terfokus dalam mengembangkan proses analisis. Dalam fase *open coding*, fase ini melibatkan pengambilan data yang diperlukan dalam penelitian. Pada penelitian ini pengambilan data dapat berupa informasi yang berasal dari website dan media sosial twitter yang diidentifikasi dengan cermat serta memastikan bahwa data yang diambil merupakan data yang relevan dengan rumusan masalah.

b) Axial Coding

Setelah fase *open coding* dilaksanakan, fase berikutnya yaitu *axial coding*. Saunders; Lewis; Thornhill. (2012) menjelaskan bahwa *axial coding* mengacu pada proses mencari hubungan antara kategori data yang berasal dari open coding. Ketika hubungan antar kategori dikenali, kemudian diatur ulang ke dalam bentuk hierarkis dan setelah itu muncul subkategori. Dalam buku Saunders; Lewis; Thornhill. (2012) mengatakan bahwa inti dari pendekatan *axial coding* adalah untuk mengeksplorasi dan menjelaskan suatu fenomena dengan mengindentifikasi apa yang terjadi dan mengapa, serta faktor yang mempengaruhi (seperti ekonomi, politik, teknologi, hukum, dan sosial budaya), yang kemudian hal tersebut dikelola dalam konteks yang

diperiksa serta hasil dari tindakan yang telah diambil.

Hal tersebut sependapat dengan Creswell (2013:85) bahwa *axial coding* muncul ketika peneliti mengidentifikasi satu kategori *open coding* yang difokuskan pada fenomena inti. Pada fase axial coding terdapat kategori – kategori yang memiliki hubungan dengan fenomena inti dalam model visual. Setelah kode dikembangkan yang berasal dari fase *open coding*, maka peneliti membaca kembali data – data yang diperoleh untuk mendapatkan pernyataan yang sesuai dengan kategori manapun, yang selanjutnya akan dimasukan ke dalam nodes yang sudah dibuat.

c) Selective coding

Creswell (2013) menjelaskan bahwa *selective coding* merupakan langkah terakhir yang dimana peneliti mengambil model dan mengembangkan proposisi yang menghubungkan kategori – kategori dalam model atau merakit sebuha cerita yang menggambarkan keterkaitan kategori dalam model. Selain itu menurut Saunders; Lewis; Thornhill. (2012:572) fase *selective coding* ini menekankan pada mengenali dan mengembangkan hubungan antara kategori utama yang muncul dari pendekatan *grounded* untuk mengembangkan teori penjelasan. Jadi fase *selective coding* merupakan langkah peneliti mengambil fenomena pusat dan menghubungkannya dengan kategori yang lain secara sistematis, yang kemudian memvalidasi hubungan tersebut serta melakukan penyempurnaan dan pengembangan secara lebih lanjut.

Pada fase ini, peneliti mendiskripiskan hubungan – hubungan yang berasal dari kategori yang sudah dibuat sebelumnya. Bermula peneliti melakukan koding data yang diperoleh yaitu data dari website dan media sosial twitter yang selanjutnya akan dimasukan ke dalam nodes. Nodes merupakan kumpulan sumber rujukan yang

berkaitan dengan topik penelitian. Informasi yang diperoleh peneliti dipastikan relevan dengan rumusan masalah yang kemudian disimpan kedalam nodes. Pada tahap terakhir, peneliti membuat *relationship* untuk menghubungkan nodes yang sebelumnya telah dibuat yang bertujuan dapat menghasilkan hubungan antar nodes.

b. Tampilan Data

Dalam penelitian kualitatif, penyajian data nya dapat disajikan dengan uraian yang singkat dan terhubung satu sama lain. Tampilan data juga dapat mempersentasikan informasi yang telah dikumpulkan dan membantu dalam penarikan kesimpulan. Saunders; Lewis; Thornhill (2012:564) menjelaskan bahwa tampilan data dapat membuat perbandingan antara elemen data dan mengidentifikasi hubungan, tema utama, pola, dan tren apapu yang terlihat. Kemudian hal ini layak untuk dieksplorasi dan dianalisis lebih lanjut. Cara ini dapat memudahkan penelitian dalah menginterpretasikan data dan setelah itu menarik makna dari hasil interpretasi. Berikut ini model tampilan data yang digunakan dalam penelitian ini, yaitu :

1) Analytical Maps

Pada penelitian ini, peneliti menggunakan *Analytical Maps* untuk membantu peneliti membuat peta analisa untuk menggambarkan konsep pemikiran yang berhubungan dengan topik. Maps yang dibuat dalam penelitian ini terbagi dalam 2 rumusan masalah diantaranya :

a) *Maps* mengenai gambaran permasalahan penipuan pada nasabah perbankan yang terdapat di Indonesia
b) *Maps* mengenai pola – pola strategi sosialisasi pencegahan penipuan *social engineering* oleh bank yang diberikan melalui media website dan media sosial twitter yang dimiliki bank – bank besar yang ada di Indonesia.

2) Matric Coding Query

Matric Coding Query dalam penelitian ini digunakan untuk melihat seberapa sering dan banyak nya antara nodes yang satu dengan yang lainnya saling berkaitan. Dalam *matrix coding query* ini akan menghasilkan hasil angka yang nantinya akan menjadi dasar untuk menganalisis perbandingan seberapa sering perbedaan penyampaian dalam pengalaman atau sikap seseorang. Fitur *query* ini cocok digunakan dalam menganalisis kecenderungan kata yang ditulis oleh seseorang dalam media sosialnya. Tidak hanya itu *matrix coding query* akan disandingkan dengan *analytical maps* yang bertujuan untuk memperjelas hubungan antara data.

a) Word Frequency

Word frequently dalam *Nvivo* ini merupakan fitur untuk mendata dan menghitung kata – kata yang paling disebut atau dapat dikatakan bahwa *word requently* ini bertujuan untuk mencari kata – kata yang sering muncul dalam satu node atau dari semua data yang ada. Jika terdapat transkrip audio dan video, maka hanya kata - kata di bagian konten (kolom) yang disertakan dalam *query*.

c. Penarikan Kesimpulan

Pada tahap ketiga dalam menganalisis data yaitu menarik kesimpulan atas data yang telah dikumpulkan, dan disajikan, yang mana tahap menarik keismpulan sebagai tahap akhir dalam menganalisis data. Tahap penarikan kesimpulan bertujuan untuk meninjau kembali hasil analis data yang sudah sesuai yang selanjutnya dikategorikan berdasarkan makna dan fungsi.

3.4.4.1 Metode Analisis Data

Metode analisis merupakan langkah penelitian dalam membahas rumusan masalah yang diikuti dengan rangkaian prosedur yang telah dispesifikasikan

sebelumnya. Metode analisis yang digunakan dalam penelitian ini adalah pendekatan *content analysist*, karena peneliti mengganggap pendekatan *content analysist* ini cocok dan tepat jika digunakan untuk menganalisis strategi pencegahan penipuan *fraud* melalui edukasi dengan menggunakan media website, media sosial twitter. Definisi *content analysist* menurut Shelley dan Krippendorff (1984) merupakan teknik penelitian untuk membantu menyimpulkan makna teks yang dapat direplikasi (replicable), dipercaya (reliable), serta teruji validitasnya. Beradasarkan definisi diatas, Shelley dan Krippendorff (1984) juga mengatakan "or other meaningful matter" yang tidak membatasi teks hanya sebatas produk tulisan, namun produk tersebut memiliki makna lain seperti lukisan, gambar, peta, suara, atau simbol.

Shelley dan Krippendorff (1984) menjelaskan bahwa terdapat tiga jenis definisi content analysist menurut para ahli :

1. Definisi analisis isi berdasarkan dari dalam teks (*definitions that take content to be inherent in a text)*
2. Definisi analisis isi yang melihat konten sebagai sumber teks *(definitions that take content to be a property of the source of a text)*
3. Definisi analisis isi berdasarkan munculnya akibat ketika peneliti melakukan proses analisa terhadap isi dalam konteks tertentu ((*definitions that take content to emerge in the process of a researcher analyzing a text relative to a particular context*)

Pada umumnya, dalam *content analysist* ada tiga pendekatan yaitu deskriptif, eksplanatif, dan predikitif. Penelitian ini berfokus pada pendekatan deskriptif yang bertujuan mendeskripsikan aspek tertentu atau karakter suatu teks. Pada pendekatan deskriptif ini tidak bertujuan untuk menguji hipotesa atau mencari

hubungan antar variable satu dengan variabel yang lainnya, namun penelitian ini berfokus pada menelaah konteks, aspek tertentu, karakter dari postingan twitter, dan situs website. Berbeda halnya dengan penelitian kuantitatif yang menganalisanya secara statistik, namun pada penelitian kualitatif ini berfokus pada mengembangkan data dengan menjelaskan atau menafsirkan ulang data kuantitatif, yang memberikan pemahaman tentang proses yang berkelanjutan (Tracy, 2013).

Dalam penelitian ini menerapkan jenis penelitian kualitatif yang menggunakan *content analysist* untuk memudahkan peneliti dalam mengelompokkan kata – kata yang bermakna sama dengan membuat kategori yang kemudian akan membangun sebuah sistem konseptual atau model. Penelitian ini menerapkan metode kualitatif yang menggunakan *content analysist*, sehingga harus melakukan prinsip – prinsip sebagai berikut :

a. Dalam menganalisa data, peneliti membaca dan menginterprestasi secara berulang terhadap tema yang dianalisis. Walaupun tujuan atau pertanyaan sudah ditentukan oleh peneliti, namun dalam analisis kualitatif hasil temuan nya berdasarkan dengan hasil analisa data mentah bukan berdasarkan asumsi, hipotesis, atau teori.
b. Dalam penelitian content analysist ini, peneliti menggunakan teknik analisis dengan mengembangkan kategori yang berasal dari data mentah yang kemudian dibuat sebuah kerangka atau model. Selanjutnya kerangka atau model ini akan berisi tema utama dan proses identifikasi serta melakukan konstruksi salama proses coding.
c. Jenis penelitian ini menggunakan penelitian kualitatif, sehingga dalam analisisnya mengutamakan interprestasi dari peneliti. Jadi hasil temuan nya berdasarkan asumsi atau *experiment* pribadi peneliti. Supaya hasil temuan nya

dapat berguna, peneliti memilah – milah data mana yang penting dan tidak penting.

d. Agar penelitian ini dapat dinilai kredibel atau teruji validitasnya dan dapat memenuhi unsur *trustworthiness*, maka peneliti melakukan proses pengkodingan *(coding consistency)* terkait prosedur di dalam penelitian.

3.4.5 Interpretasi Data

Setelah selesai pada proses mengurutkan, mengelompokkan, mereduksi dalam analisa data, maka selanjutnya peneliti melakukan proses interpretasi data. Interpretasi data merupakan proses meninjau kembali data yang sudah dikumpulkan dan dianalisis untuk membantu peneliti dalam memberikan makna pada data, sehingga dapat menghasilkan kesimpulan yang relevan. Dengan adanya interpretasi data, dapat memudahkan pembaca dalam memahami grafik, tabel, teks, diagram, serta model lainnya. Dengan demikian, dalam proses ini diperlukan untuk berfikir kritis dalam memberi kesimpulan atas informasi yang telah didapatkan selama penelitian.

3.5 Objek Penelitian

Objek penelitian yang digunakan berfokus pada media sosial *twitter* dan situs resmi (website) 6 perusahaan perbankan terbesar di Indonesia yaitu Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI).

3.6 Instrumen Penelitian

Putra (2011) mengatakan bahwa instrument utama dalam penelitian kualitatif adalah peneliti itu sendiri. Lebih lanjut Creswell (2013) berpendapat bahwa instrument kunci dalam penelitian kualitatif adalah peneliti, peneliti kualitatif yang mengumpulkan data sendiri dengan cara memeriksan dokumen,

mengamati perilaku, dan mewancarai partisipan. Maka dari itu, peneliti memiliki peranan yang penting dalam menjalankan proses penelitian dan mengambil data yang diperlukan. Selain itu instrument yang diperlukan dalam penelitian ini adalah laptop yang berguna untuk mencari data di media website dan media sosial twitter perusahaan perbankan, serta peneliti menggunakan software *NVivo 12 plus* untuk membantu proses penelitian. Software *NVivo 12 plus* merupakan software untuk menganalisis data kualitatif yang dikembangkan oleh *Qualitative Solution and Research (QSR) International*. QSR merupakan sebuah perusahaan yang mengembangkan software untuk menganalisis data kualitatif. Software *Nvivo* merupakan perangkat lunak yang didesain dengan *Qualitative Data Analysis* yang mudah digunakan untuk menghimpun, mengelompokkan atau memetakan data serta proses analisa dan pengolahan data.

3.7 Pengujian Keabsahan Data

Pengujian keabsahan data dalam penelitian sudah tidak dapat dipisahkan, karena uji keabsahan data memiliki tujuan untuk menentukan konsep penelitian kualitatif yang digunakan bersifat ilmiah atau tidak, serta untuk menguji data yang telah diperoleh. Berdasarkan data yang telah terkumpul, tahap selanjutnya peneliti melakukan pengujian keabsahan data. Pada penelitian ini, teknik keabsahan data yang digunakan meliputi uji kredibilitas dan uji dependebilitas

3.7.1 Uji Kredibilitas

Pada penelitian kualitatif, data yang dapat disebut kredibel ketika data tersebut memiliki kesesuaian antara data yang dilaporkan oleh peneliti dengan data yang sesungguhnya terjadi. Dalam penelitian ini pengujian kredibelitas menggunakan teknik triangulasi. Hancock dan Algozzine (2006:87) mengatakan

triangulasi merupakan penerapan dan kombinasi dari beberapa penelitian metodologi penelitian dalam mempelajari fenomena yang sama. Teknik triangulasi merupakan konsep metodelogis yang bertujuan untuk menguatkan tingkat teoritis, metodologis, ataupun interpretatif untuk penelitian kualitatif.

Pada penelitian ini, tringulasi yang digunakan untuk melakukan pengecekan data adalah triangulasi sumber yang berfokus pada data yang diperoleh dari berbagai sumber. Jika teknik triangulasi sumber dikaitkan dengan penelitian ini tentang sosialisasi pencegahan penipuan *social engineering* pada nasabah bank, maka pengujian keabsahan data yang diperoleh dapat dilakukan dengan mencari informasi yang bersumber dari situs website resmi dan media sosial yang dimiliki bank seperti Twitter dan tentunya sudah tervaliditas.

Dengan adanya berbagai sumber dalam memperoleh data, hal ini dapat memudahkan peneliti dalam membandingkan data satu dengan yang lain. Selain itu, tidak hanya dari situs website resmi dan media sosial twitter bank untuk memperoleh data, namun peneliti juga menggunakan dokumen yang lainnya sebagai penunjang penelitian yaitu hasil statistik tingkat kejahatan penipuan pada nasabah, Perarturan Perundang – Undangan yang mengatur kewajiban bank untuk melindung nasabahnya. Data yang diperoleh dari tiga sumber tersebut tidak dapat dirata – rata kan seperti yang dilakukan pada penelitian kuantitatif, melainkan dalam penelitian kualitatif data tersebut dideskripsikan , dikategorisasikan dengan berlebih spesifik. Kemudian dari data yang sudah melalui proses analisis , dapat dilanjutkan dengan proses penarikan kesimpulan.

3.7.2 Uji Dependabilitas

Pengujian dependabilitas dalam penelitian kualitatif dapat disebut dengan pengujian reliabilitas. Pengujian dependabilitas dapat dilakukan dengan kegiatan pemeriksanaan pada seluruh proses penelitian. Penelitian yang dapat dikatakan *dependable* adalah ketika peneliti dapat menunjukkan bahwa penelitian yang dilakukan adalah nyata dengan melalui rangkaian proses penelitian. Supaya sebuah penelitian kualitatif dapat memenuhi kriteria dapat dipercaya *(trustworthiness)*, maka dapat dilakukan dengan meninjau kembali hasil analisis dengan ahli nya *(expert review)*. Maka dalam penelitian ini mekanisme pengujian dependalibilitas dilakukan dengan berkonsultasi pada dosen pembimbing secara berkelanjutan, untuk memberikan bimbingan serta penilaian terkait dengan proses coding hingga hasil nya relevan dengan tujuan penelitian.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengenalan Bab

Bab ini akan menjelaskan serangkain temuan yang didapatkan dalam proses penelitian, yang berguna menjawab setiap rumusan masalah yang sebelumnya telah disusun oleh peneliti. Tahapan pertama, yang dilakukan oleh peneliti adalah melakukan koding atas informasi yang telah di capture menggunakan *NCapture* yang didapatkan dari situs website resmi bank, media sosial twitter bank, serta berita online yang relevan dengan rumusan masalah untuk kemudian dianalasis. Tahap kedua, mengklasifikasikan data sesuai dengan pembahasan jawaban atas rumusan masalah. Pada bab ini diawali dengan membahas profil singkat dari bank – bank yang menjadi objek penelitian diantaranya Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI). Selanjutnya peneliti akan menjelaskan rangkaian rumusan masalah, diantaranya yang pertama membahas terkait gambaran permasalahan penipuan *social engineering* pada nasabah bank - bank yang terdapat di Indonesia. Kedua, membahas pola – pola strategi sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh bank melalui media website dan media sosial twitter yang dimiliki bank – bank besar yang ada di Indonesia. Ketiga membahas mengenai perbaikan yang sebaiknya dilakukan oleh perusahaan perbankan dalam rangka peningkatan sosialisasi di media website dan media sosial twitter.

4.2 Gambaran Umum Perusahaan Perbankan di Indonesia

4.2.1 PT. Bank Mandiri (Persero) Tbk

a. Profil PT. Bank Mandiri (Persero) Tbk

PT. Bank Mandiri Tbk merupakan salah satu Badan Usaha Milik Negara (BUMN) yang berdiri tanggal 2 Oktober 1998. Bank Mandiri berdiri sebagai bagian dari program restruksasi perbankan yang dilaksanakan oleh pemerintah Indonesia terhitung pasca merger dari Bank Dagang Negara, Bank Bumi Daya, Bank Ekspor Impor Indonesai, dan Bank Pembangunan Indonesia. Bank Mandiri bergerak di bidang perbankan yang fungsinya sebagai badan usaha yang menghimpun dana dari masyarakat dan menjadi fasilitator transaksi keuangan. Asset Bank Mandiri yang seiring bertumbuh sampai dengan Rp 1.725,6 triliun di tahun 2021 silam. Berdasarkan laporan tahunan Bank Mandiri 2021, total kantor cabang dalam negri perseroan sebanyak 2.602 dengan tersebar 37.840 karyawan. Dalam rangka mengatasi persaingan perbankan, Bank Mandiri bertekad untuk memberikan solusi keuangan yang luas dan memberikan standar layanan yang bertujuan untuk meningkatkan rasa nyaman dan kepuasan terhadap nasabah.

b. Visi dan Misi PT. Bank Mandiri (Persero) Tbk

Berdasarkan *sustainability report* bank mandiri tahun 2021, Bank Mandiri memiliki visi jangka panjang 2020-2024 yaitu “Menjadi Partner Finansial Pilihan Utama Anda” yang sesuai dengan tujuan mereka “Spirit Memakmurkan Negeri”. Berikut penjelasan Visi Bank Mandiri :

1. Komitmen membangun hubungan jangka Panjang yang berlandaskan kepercayaan nasabah bisnis dan perorangan. Bank Mandiri melayani seluruh nasabah dengan standar layanan internasional melalui penyediaan solusi

keuangan yang inofatif. Bank Mandiri ingin dikenal karena kinerja, sumber daya manusia dan kerja sama tim yang terbaik.

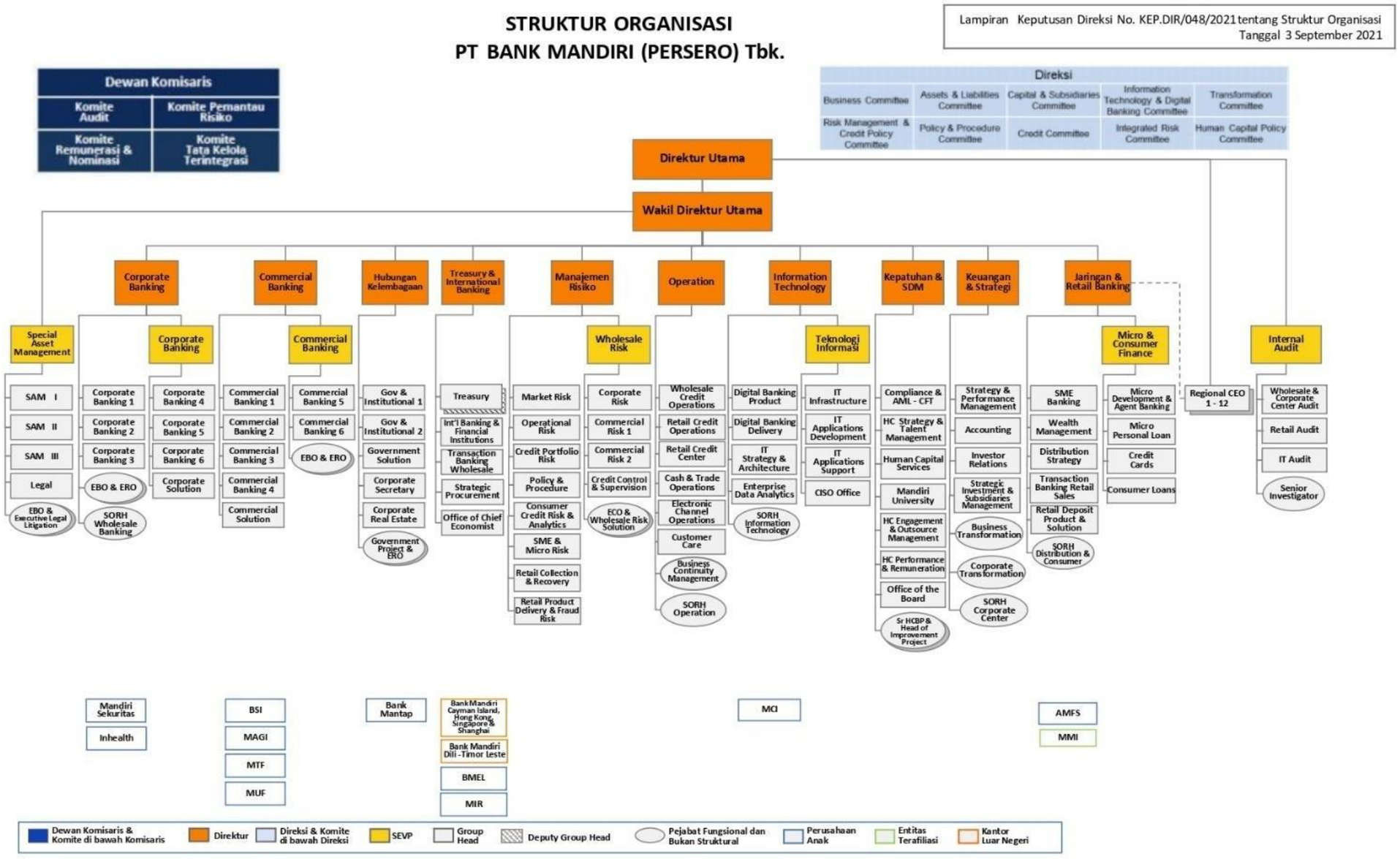
2. Mengambil peran aktif dalam mendorong pertumbuhan ekonomi jangka Panjang Indonesia dan selalu menghasilkan imbal balik yang tinggi secaea konsisten bagi pemegang saham.

Misi Bank Mandiri yang dilansir *sustainability report* Bank Mandiri tahun 2021 yaitu "Menyediakan Solusi Perbankan Digital Yang Handal Dan Praktis Yang Menjadi Bagian Hidup Nasabah". Hal ini sesuai dengan tema program kerja budaya Bank Mandiri diantaranya :

1. Satu hati satu Mandiri
2. Mandirian tangguh
3. Tumbuh sehat
4. Memenuhi kebutuhan pelanggan
5. Bersama membangun Negeri

c. Struktur Organisasi Perusahaan

Gambar IV. 1 Struktur Organisasi PT. Bank Mandiri (Persero) Tbk



Sumber : bankmandiri.co.id

4.2.2 PT. Bank Central Asia Tbk.

a. Profil PT. Bank Central Asia Tbk.

PT. Bank Central Asia Tbk. merupakan bank swasta terbesar di Indonesia yang didirakan pada 10 Oktober 1955. Bank BCA memiliki fokus pada bisnis perbankan transaksi dan memberikan fasilitas kredit dan solusi keuangan yang diperutunkkan bagi korporasi, komersial, UKM, serta konsumer. Berdasarkan situs website resmi Bank BCA pada akhir Maret 2022 telah melayani lebih dari 29 juta nasabah, yang didukung dengan kantor cabang sejumlah 1.241. Selain itu Bank BCA memiliki asset Rp 1.259 triliun dengan laba bersih Rp. 8,1 Triliun.

b. Visi dan Misi PT. Bank Central Asia Tbk.

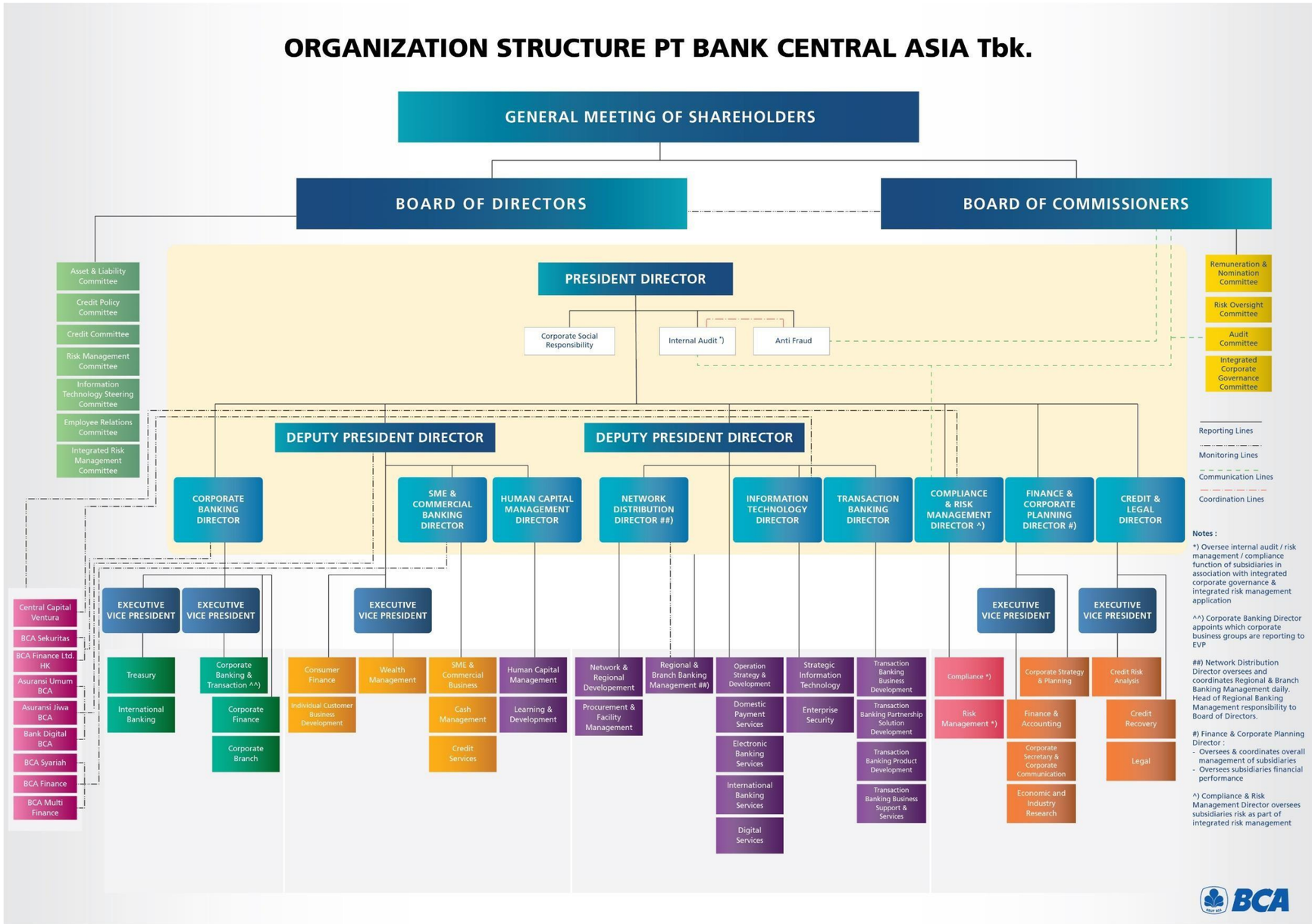
Berdasarkan laporan tahunan PT. Bank Central Asia Tbk. tahun 2021, Bank Central Asia memiliki visi sebagai "Bank Pilihan Utama Andalan Masyarakat, Yang Berperan Sebagai Pilar Penting Perekonomian Indonesia". Dalam rangka melanjutkan visi tersebut, Bank BCA memiliki misi diantaranya :

1. Membangun institusi yang unggul di bidang penyelesaian pembayaran dan solusi keuangan bagi nasabah bisnis dan perseorangan
2. Memahami beragam kebutuhan nasabah dan memberikan layanan finansial yang tepat demi tercapainy kepuasan optimal bagi nasabah
3. Meningkatkan nilai francais dan nilai stakeholder BCA

Hal tersebut sesuai dengan tata nilai yang dimiliki oleh PT. Bank Central Asia Tbk. yaitu fokus pada nasabah, integritas, kerjasama tim, berusaha mencapai yang terbaik.

c. Struktur Organisasi

Gambar IV. 2 Struktur Organisasi PT. Bank Central Asia Tbk



Sumber : bca.co.id

4.2.3 PT. Bank Rakyat Indonesia (Persero) Tbk.

a. Profil PT. Bank Rakyat Indonesia (Persero) Tbk.

PT. Bank Rakyat Indonesia (Persero) Tbk. merupakan salah satu bank tertua milik BUMN di Indonesia. Bank Rakyat Indonesia (BRI) didirikan oleh Raden Bei Aria Wirjaatmadja tahun 1895 yang awalnya dengan nama *De Poerwokertosche Hulp en Spaarbank der Inlandsche Hoofden* atau "Bank Bantuan dan Simpanan Milik Kaum Priyayi Purwokerto". Bank Rakyat Indonesia (BRI) awalnya suatu Lembaga keuangan yang memberikan layanan kepada orang – orang pribumi. Aset yang dimiliki BRI per 31 Desember 2021 tercatat Rp. 1.678,10 triliun. BRI juga konsisten dalam mengembangkan layanan Micro Banking bagi kalangan Usaha Mikro, Kecil, dan Menengah (UMKM) melalului lebih dari 10.000 unit kerja yang terintegrasi secara online di seluruh Indonesia.

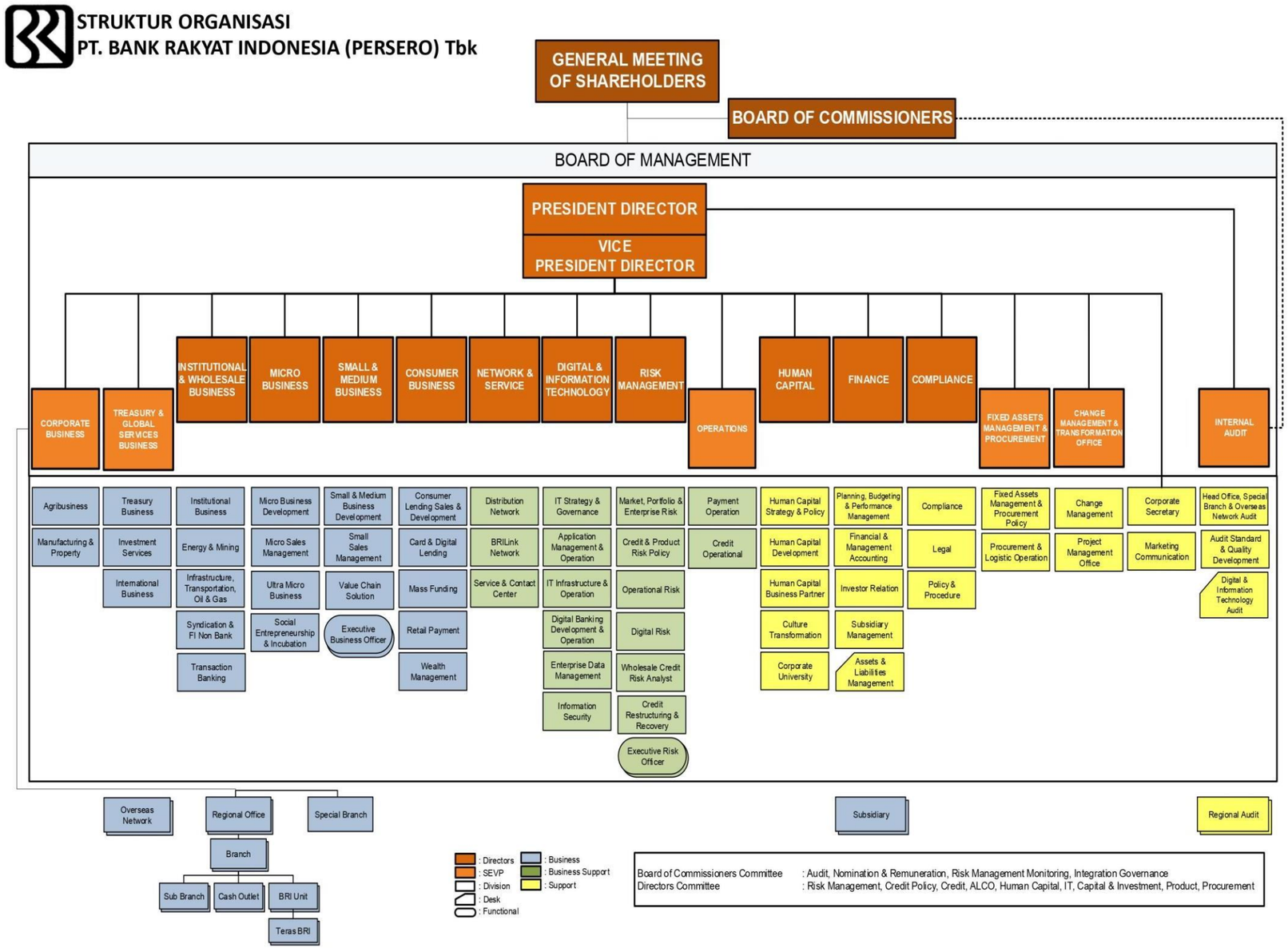
b. Visi dan Misi PT. Bank Rakyat Indonesia (Persero) Tbk.

Dalam rangka memajukan perusahaan, BRI memiliki visi menjadi “The Most Valuable Banking Group di Asia Tenggara dan Champion of Financial Inclusion”. Dalam merealisasikan visi tersebut, Bank Rakyat Indonesia (BRI) memiliki misi diantaranya :

1. Memberikan yang terbaik
2. Menyediakan pelayanan yang prima
3. Bekerja dengan optimal dan baik

c. Struktur Organisasi

Gambar IV. 3 Struktur Organisasi BRI



Sumber : bri.co.id

4.2.4 PT. Bank Negara Indonesia (Persero) Tbk.

a. Profil PT. Bank Negara Indonesia (Persero) Tbk.

BNI merupakan Bank Badan Usaha Milik Negara (BUMN) pertama yang menjadi perusahaan publik setelah mencatatkan sahamnya di Bursa Efek Jakarta dan Bursa Efek Surabaya pada tahun 1996. Layanan yang diberikan BNI diantaranya penyimpanan dana maupun fasilitas pinjaman pada segmen korporasi ditingkat menengah, maupun kecil. Produk yang diberikan oleh BNI telah sesuai dengan kebutuhan yang diperlukan oleh nasabah semenjak kecil, remaja, bertumbuh dewasa, hingga nasabah pensiun. Selain itu, BNI semakin menigkatkan bisnisnya yang terlihat pada asset yang meningkat di tahun 2021 yaitu sejumlah Rp. 964 triliun.

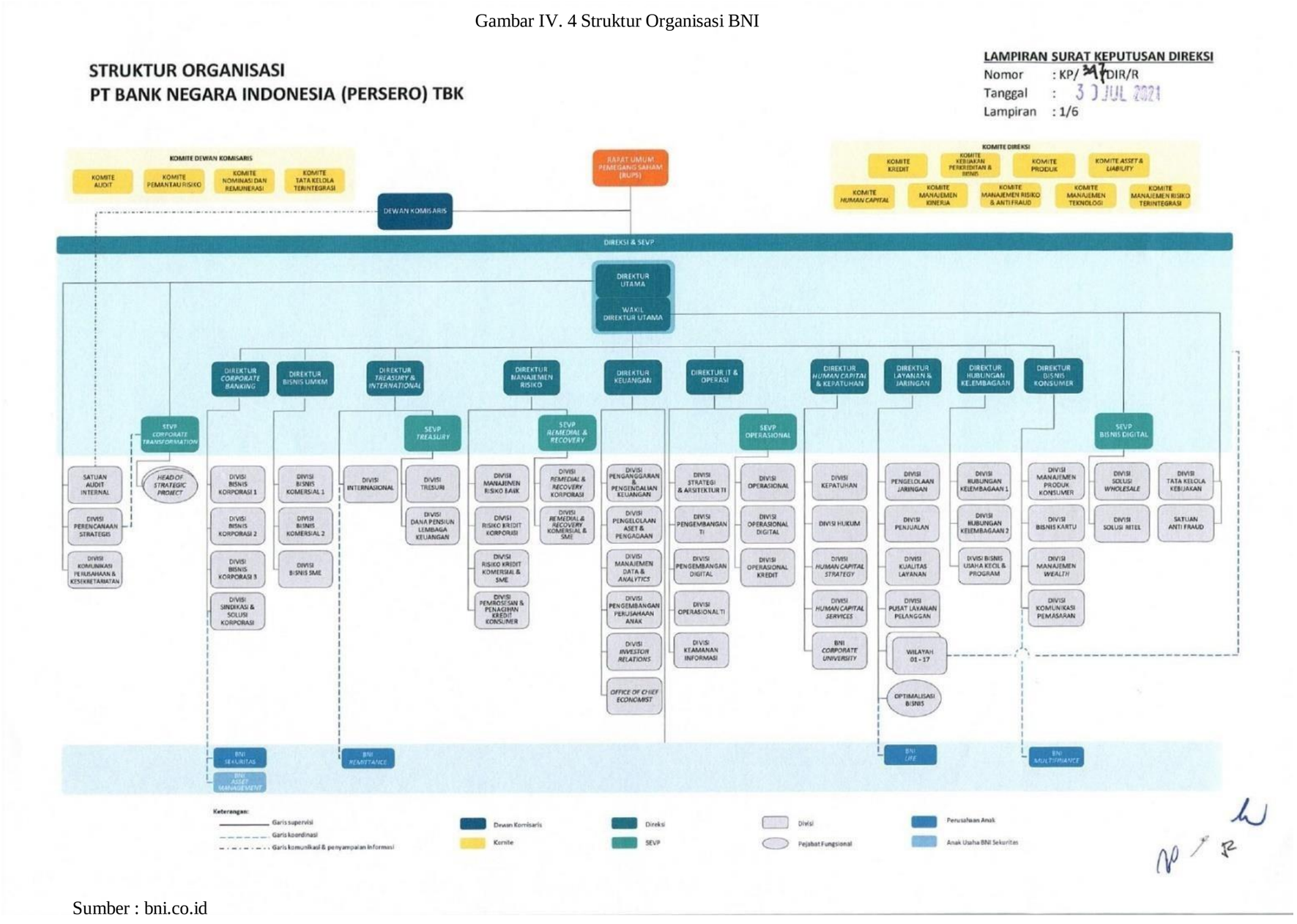
b. Visi dan Misi PT. Bank Negara Indonesia (Persero) Tbk.

Sebagai upaya mempertahankan posisinya sebagai Bank yang terkemuka, BNI memiliki visi untuk menentukan langkah ke depan yaitu "Menjadi Lembaga Keuangan Yang Terunggul Dalam Layanan dan Kinerja Secara Berkelanjutan". Agar dapat mencapai visi tersebut, BNI memiliki misi untuk merealisasikan nya, yaitu :

1. Memberikan layanan prima dan solusi digital kepada seluruh nasabah selaku mitra bisnis pilihan utama.
2. Memperkuat layanan internasional untuk mendukung kebutuhan mitra bisnis global.
3. Meningkatkan nilai investasi yang unggul bagi investor.
4. Menciptakan kondisi terbaik bagi karyawan sebagi tempat kebanggan untuk berkarya dan berprestasi.
5. Meningkatkan kepedulian dan tanggung jawab kepada lingkungan dan masyarakat.
6. Menjadi acuan pelaksanaan kepatuhan dan tata keloal perusahaan yang baik bagi industri.

c. Struktur Organisasi PT. Bank Negara Indonesia (Persero) Tbk.

Gambar IV. 4 Struktur Organisasi BNI



Sumber : bni.co.id

4.2.5 PT. Bank Permata Tbk

a. Profil PT. Bank Permata Tbk

Bank Permata merupakan salah satu bank yang telah terdaftar di Bursa Efek Indonesia (BEI) dan termasuk kategori bank BUKU 4. Pada awalnya Bank Permata Bernama Bank Persatuan Dagang Indonesia yang berdiri pada 17 Desember 1954. Berdasarkan situs website Bank Permata, Bank Permata menawarkan rangkaian lengkap produk dan jasa perbankan diantaranya rekening giro dan tabungan, deposit berjangka, reksa dana, obligasi, pinjaman perorangan, kartu kredit dan hipotek untuk konsumen retail yang tersedia dalam konvensional dan syariah. Dalam rangka mengembangkan bisnisnya, Pada September 2021 Bank Permata memiliki 291 kantor cabang dan telah melayani leboh dari 4,2 juta konsumen. Akhir tahun 2021 Bank Permata mencatat pertumbuhan asset sebesar Rp. 234 triliun dan berhasil membukukan laba bersih setelah pajak sebesar Rp. 1,2 triliun.

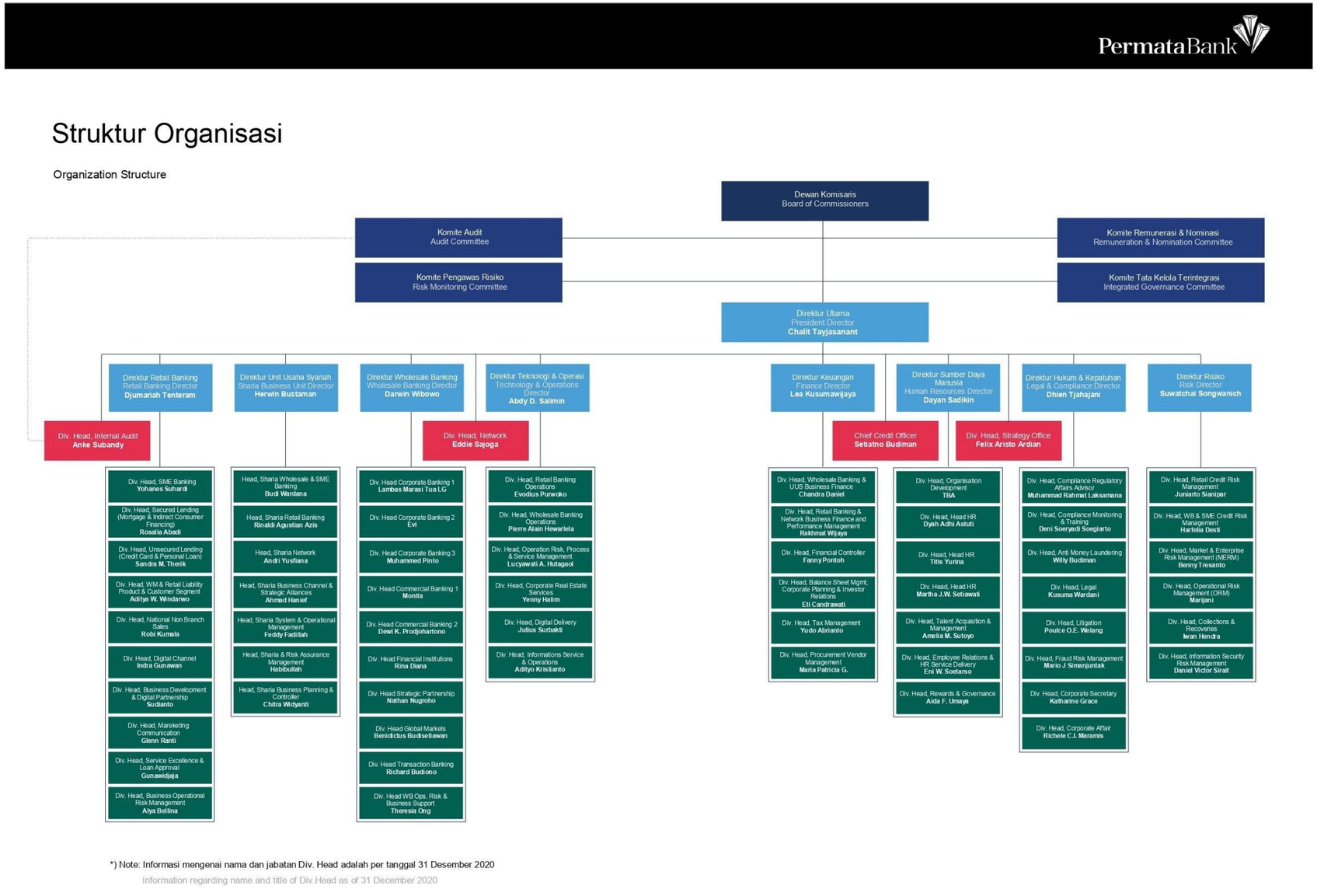
b. Visi dan Misi PT. Bank Permata Tbk

Semakin berkembangnya PT. Bank Permata Tbk, tentunya memiliki visi yang jelas untu menentukan langkah kedepan nya. Ban Permata memiliki visi “Menjadi Bank Pilihan Dengan Terus Membina Kemitraan dan Menciptakan Nilai Bermakna Bagi Stakeholder”. Dalam melanjutkan visi tersebut, Bank Permata memiliki misi diantaranya :

1. Berperan aktif sebagai mitra di bidang keuangan dan agen pembangunan yang efisien bagi nasabah dan masyarakat.
2. Memberikan layanan keuangan menyeluruh secara sederhana, cepat, andal, dan inovatif.
3. Berkomitmen untuk memberikan pengalaman unggul bagi pemangku kepentingan dan membangun nilai positif bagi pemegang saham.

c. Struktur Organisasi PT. Bank Permata Tbk

Gambar IV. 5 Struktur Organisasi Bank Permata



Sumber : permatabank.com

4.2.6 PT. Bank Syariah Indonesia Tbk

a. Profil PT. Bank Syariah Indonesia Tbk

PT. Bank Syariah Indonesia Tbk merupakan bank di Indonesia yang bergerang dalam bidang perbankan yang berbasis syariah. BSI berdiri pada 1 Februari 2021 yang merupakan hasil penggabungan Bank Syariah Mandiri, BNI Syariah, dan BRI Syariah yang menjadi satu. Penggabungan dari ketiga bank ini menghadirkan layanan yang lebih lengkap, jangkauan yang lebih luas, serta memiliki kapasitas permodalan yang lebih baik karena didukung sinergi oleh perusahaan induk yaitu Bank Mandiri, BNI, BRI serta Pemerintah melalui Kementrian BUMN. Hal ini, dapat mendorong Bank Syariah Indonesia untuk dapat bersaing di tingkat global. Hadirnya Bank Syariah Indonesia menjadi cerminan wajah perbankan yang berbasis syariah dan modern, universal, dan memberikan kebaikan bagi segenap alam (Rahmatan Lil'Aalamiin). Selain itu, Bank Syariah Indonesia menjadi bank syariah milik Himpunan Bank Milik Negara (HIMBARA).

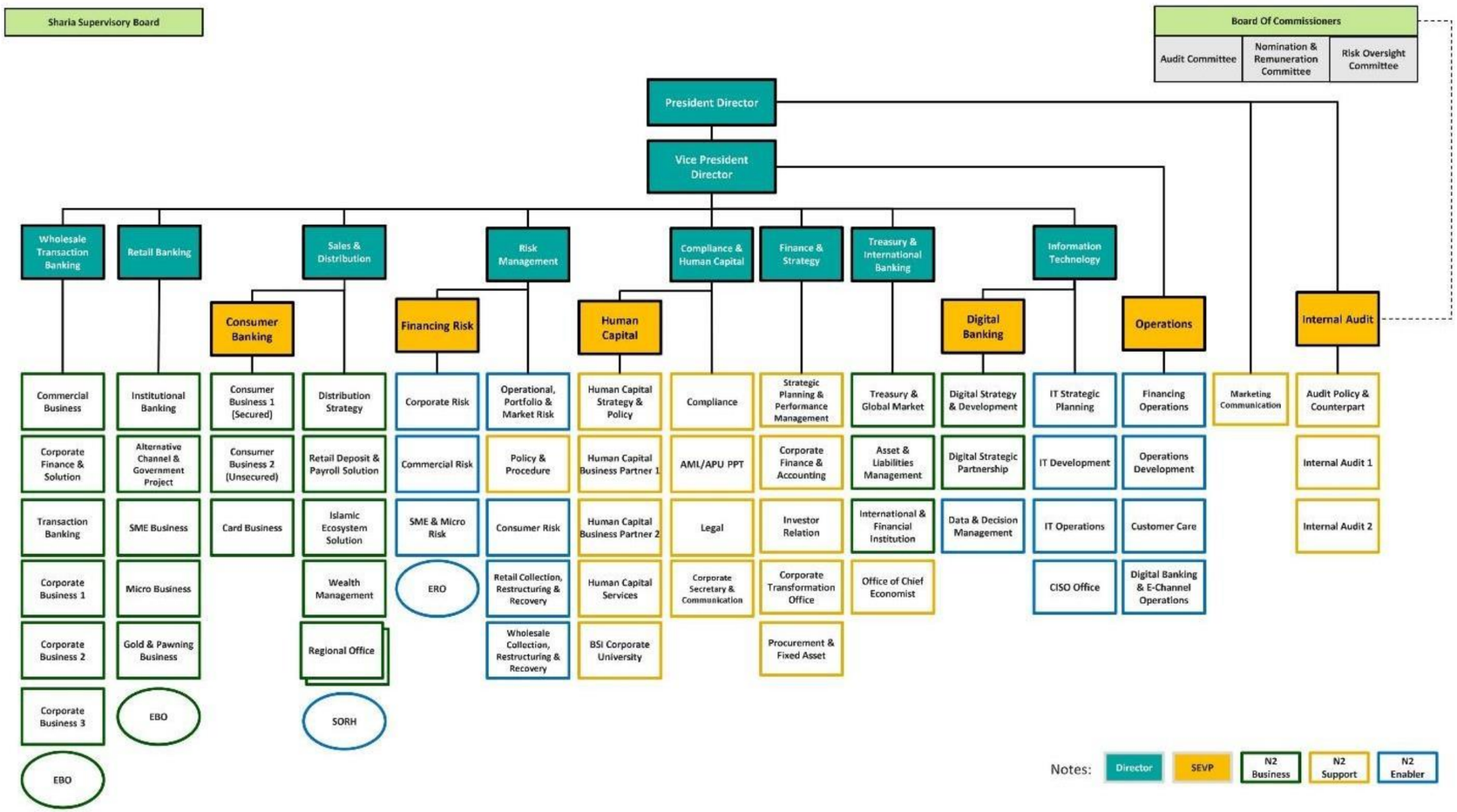
b. Visi dan Misi PT. Bank Syariah Indonesia Tbk

Bank Syariah Indonesia memiliki peran penting sebagai fasilitator pada seluruh aktivitas ekonomi di dalam ekosistem industri halal. Dalam rangka mengembangkan perusahaan nya, Bank Syariah Indonesia memiliki visi untuk menentukan langkah ke depan yaitu "Top 10 Global Islamic Bank". Visi tersebut dilanjutkan dengan misi sebagai berikut :

1. Memberikan akses solusi keuangan syariah di Indonesia.
2. Menjadi bank besar yang memberikan nilai terbaik bagi para pemegang saham.
3. Menjadi perusahaan pilihan dan kebanggaan para talenta terbaik Indonesia.

c. Struktur Organisasi PT. Bank Syariah Indonesia Tbk

Gambar IV. 6 Struktur Organisasi Bank Syariah Indonesia



Sumber : bankbsi.co.id

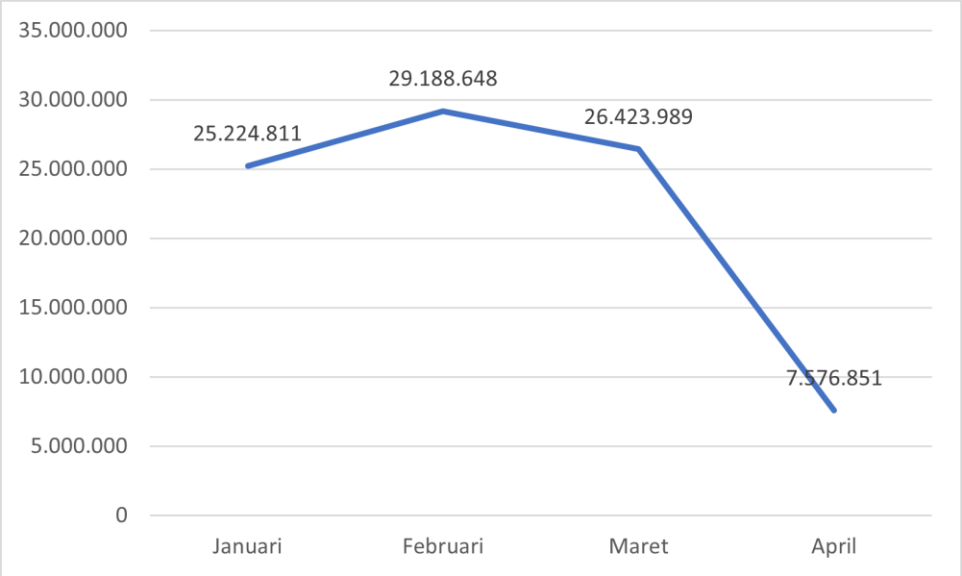
4.3 Gambaran Permasalahan Penipuan *Social Engineering* Pada Nasabah Bank - Bank Yang Terdapat Di Indonesia

Pandemi COVID-19 memiliki dampak bagi aktivitas masyarakat yaitu membentuk sebuah budaya melakukan aktivitas secara online. Hal ini disebabkan adanya kebijakan Pemerintah yang dilakukan secara gencar untuk mendukung gerakan *Stay at Home*, dan kegiatan ini dilakukan sebagai upaya penurunan kasus penularan virus *Corona*. Kondisi pandemi ini tentunya memiliki dampak bagi semua sektor, terkhususnya sektor perbankan.

Dalam sektor perbankan, khususnya Bank tentunya harus melakukan inovasi terbaru agar dapat bersaing di industri perbankan. Salah satunya adalah melakukan segala aktivitas dapat dilakukan secara online, yaitu dengan menyediakan *e-banking*, online *payment point, sms banking*, dan lain – lain yang memudahkan nasabah dalam bertransaksi tanpa keluar rumah.

Aktivitas online semakin mudah untuk dilakukan karena seiring berkembangnya teknologi yang menggunakan internet. Hal ini, membuat aktivitas masyarakat selalu mengandalkan internet. Namun, penggunaan internet memiliki dampak negative yaitu rawan terhadap penipuan, sehingga masyarakat harus lebih berwaspada terhadap kejahatan di dunia siber *(cybercrime)*.

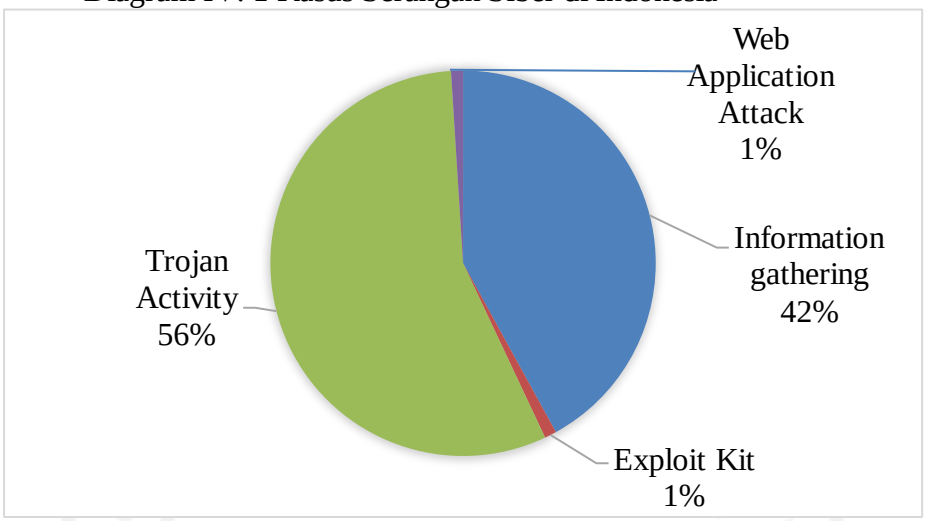
Gambar IV. 7 Data Serangan Siber di Indonesia



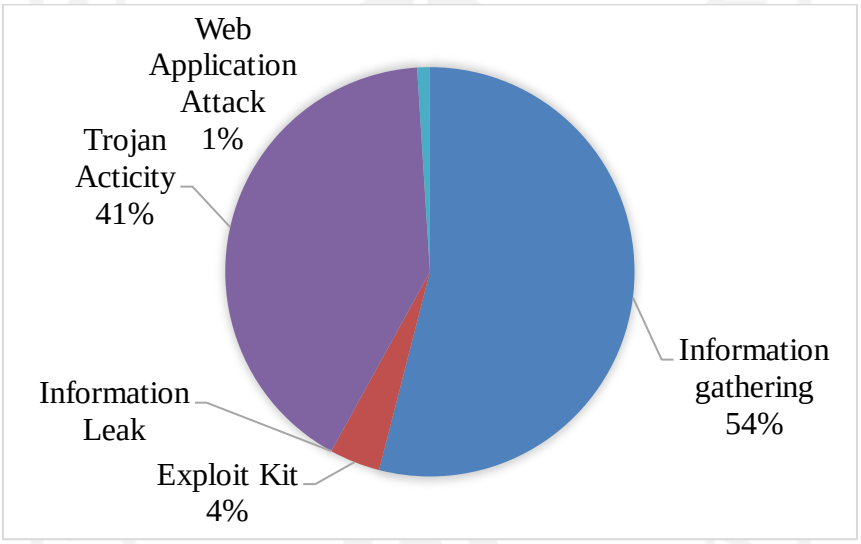
Sumber BSSN : Diolah peneliti *) per 1 Januari – 12 April 2020

Menurut Badan Siber dan Sandi Negara (2020) pada tanggal 1 Januari hingga 12 April 2020 tercatat sebesar 88.414.296 serangan siber yang terjadi. Tercatat 25.224.811 serangan pada bulan Januari, terpantau 29.188.645 serangan pada bulan Februari, terdapat 26.423.989 serangan pada bulan Maret, dan bulan 12 April terpantau 7.576.851 serangan. Berdasarkan data Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) serangan yang terjadi berjenis *Malicious Email Phising dengan isu pandemic Covid-19 sebagai latar belakang penyerangan.* Serangan ini mempengaruhi psikologi dan mengeksploitasi kelemahan korban dari sebuah keamanan, teknik penipuan ini disebut dengan *social engineering.*

Diagram IV. 1 Kasus Serangan Siber di Indonesia



*) Bulan Maret



*) Bulan April

Sumber : BSSN

Pada data sebelumnya dijelaskan mengenai grafik serangan siber dari bulan 1 Januari hingga 12 April, selanjutnya akan diperinci lagi jenis serangan *cyber crime* yang terjadi. Peneliti mengambil data pada bulan Maret dan April untuk membandingkan kenaikan persentasi tiap kasus nya. Pada bulan April 2020 didominasi oleh kasus *information gathering* yang hal ini termasuk serangan *social engineering*. *Information gathering* adalah keinginan untuk mengetahui lebih banyak tentang informasi calon korban. Kasus *information gathering* pada bulan April memiliki persentase 54%, yang hal ini

menunjukkan bahwa terjadi kenaikan dari bulan sebelumnya yaitu 42%.

BSSN mencatat terdapat lebih dari 1,65 miliar anomaly trafik keamanan siber pada Januari – Desember 2021. Hal tersebut disampaikan oleh Wakil Kepala BSSN Irjen Luki Hermawan pada acara *Launching* Laporan Tahunan Monitoring Kemanaan Siber.

"Kami memantau dari hasil monitoring di sepanjang 2021 ada ancaman anomaly trafik yang besar sekali, yaitu lebih dari 1,65 miliar serangan siber," (Irjen Luki Hermawan,2022)

Irjen Luki Hermawan mengungkapkan total *anomaly trafic* tersebut paling banyak berasal dari infeksi malware 62%, aktivitas trojan 10% dan information gathering 9%, sisanya tren kasus insiden siber di Indonesia berupa *web defacements, data breach, human operated ransomware, advance persistent threat, phising*. Dengan demikian, persentase infeksi malware yang tinggi pada anomaly trafik akan menyebabkan munculnya indikasi pencurian informasi menjadi tinggi di setiap aktivitas masyarakat.

Serangan siber juga meluas ke industri keuangan, hal ini disampaikan oleh OJK. Tercatat pada tahun 2021 terdapat serangan siber pada 10 besar industri yaitu sebanyak 22,4% yang terjadi di sektor keuangan. Dengan perincian 70% serangan yang ditujukkan pada sektor perbankan, 16% perusahaan asuransi, dan 14% sektor keuangan lainnya. Dengan demikian serangan siber di sektor keuangan akan diprediksikan mengalami peningkatan, sesuai dengan konfersi pers dari pihak OJK:

"Probabilitas serangan siber di sektor keuangan ke depan diprediksikan bisa mencapai 86,7% dan memang diprediksikan akan sukses apabila bank – bank tidak siap untuk

melakukan mitigasi kepada keamanan siber" (Deputi Direktur Basel dan Perbankan Internasional, Departemen Penelitian dan Pengaturan Perbankan OJK Tony, 2022).

Saladin D Effendi selaku *Chief Information Security Officer* Bank Mandiri di konfersi pers yang sama juga mengatakan:

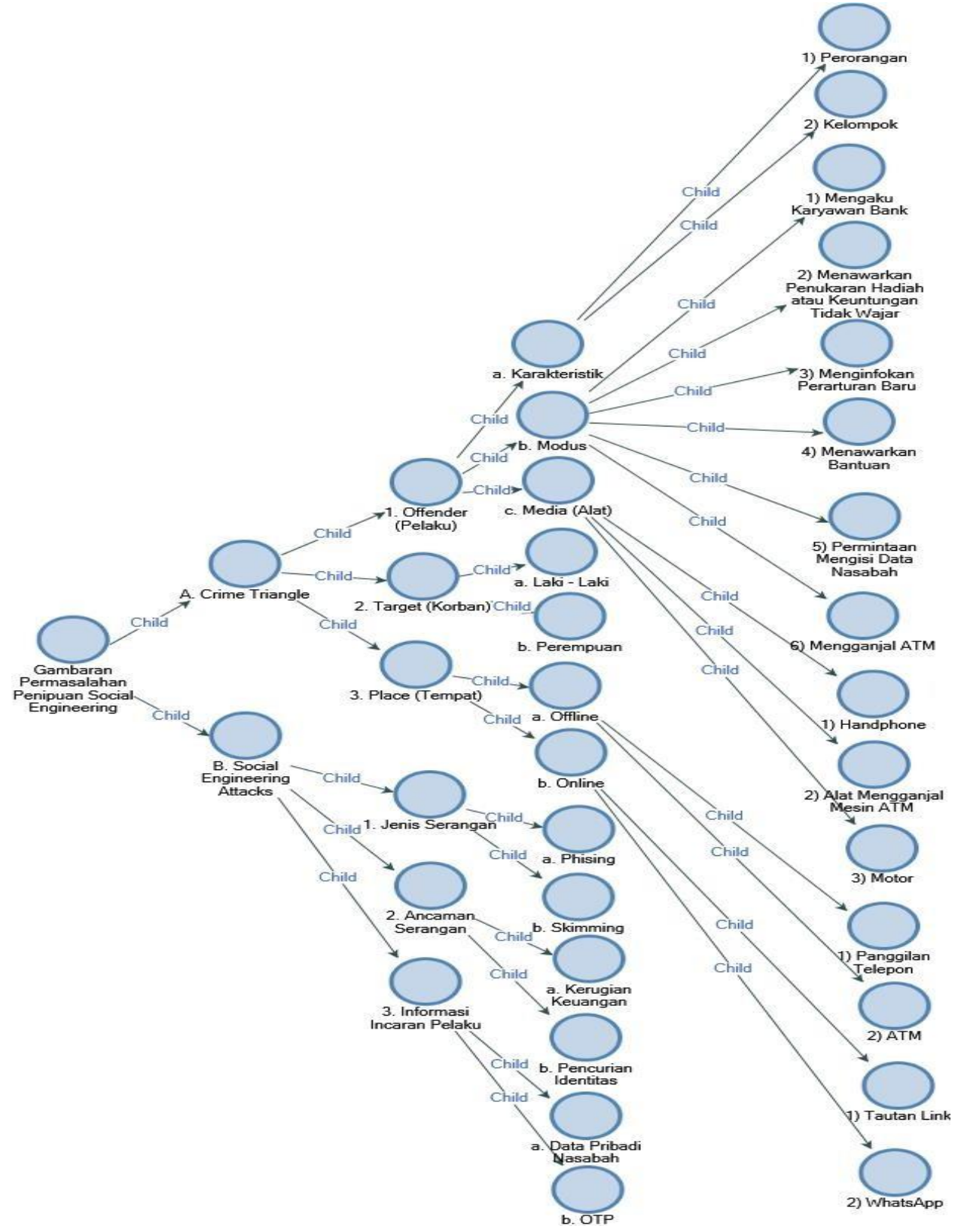
"Digitalisasi yang terus berkembang dalam memberikan kenyamanan nasabah, tentu dibarengi dengan ancaman risiko serangan. Hal tersebut tentu harus diantisipasi oleh perbankan."(Saladin D Effendi,2022).

Selain itu Saladin D Effendi menambahkan terdapat tiga ancaman kejahatan siber teratas secara global di tahun 2022, yaitu *social engineering dan ransomware, identity dan access control attack, serta supply chain attack.* Kasus *social engineering* dan *ransomware* awalnya disebabkan oleh orang – orang yang sering berkerja dari rumah dan sering mengklak – klik sesuatu, dan pada akhirnya terjebak pada *phising* email yang diklik. Hal ini yang kemudian akan mengaktifkan *ransomware*, sesuai dengan konfersi pers yang disampaikan oleh *Chief Information Security Officer* Bank Mandiri :

"Kemudian *ransomware* dari 2020 ke 2021 itu meningkatkan 435%, karena sekarang sudah ada *service*-nya yang bisa di-download, bisa diambil, bisa nyerang. Ini yang jadi threat nomor satu, threat keduanya itu *identity* dan *access control attack*, dan *threat* ketiga itu *supply chain attack*," (Saladin D Effendi,2022)

Selanjutnya peneliti akan menguraikan terkait gambaran permasalahan penipuan *social engineering* yang akan dihubungkan dengan teori *the crime triangle* (segi tiga kejahatan) yang divisualisasikan dengan peta analisa yang menggunakan *software NVIVO 12* yang tunjukkan pada gambar IV.8 .

Gambar IV.8 Peta Analisa Gambaran Permasalahan Penipuan *Social Engineering*



Sumber : Diolah Peneliti Menggunakan Software NVivo 12

Tabel IV. 1 Matrix Coding Query Gambaran Permasalahan Penipuan *Social Engineering* (Berdasarkan Jumlah Kata)

Gambaran Permasalahan Penipuan *Social Engineering*	Polda Aceh	Polda Bengkulu	Polda DIY	Polda Metro Jakarta Barat	Polda Metro Jaya	Polda Sulut	Polres Depok	Polres Jepara	Polres Kobar	Polres Lumajang	Polres Pasuruan	Polres Trenggalek	Polresta Padang	Polresta Sidoarjo
A. *Crime Triangle*	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1. *Offender* (Pelaku)	No	No	No	No	No	No	No	No	No	No	No	No	No	No
a. Karakteristik	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1) Perorangan	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	No
2) Kelompok	No	Yes	Yes	No	Yes	Yes	No	Yes	No	No	Yes	No	No	Yes
b. Modus	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1) Mengaku Karyawan Bank	Yes	No	Yes	No	Yes	No	No	No	No	No	No	Yes	No	No
2) Menawarkan Penukaran Hadiah atau Keuntungan Tidak Wajar	Yes	No	Yes	Yes	Yes	No	No	No	Yes	No	No	No	No	No
3) Menginfokan Perarturan Baru	No	No	Yes	No	No	No	No	No	No	No	No	No	No	No
4) Menawarkan Bantuan	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	Yes
5) Permintaan Mengisi Data Nasabah	Yes	No	No	No	Yes	No	No	No	No	No	No	No	Yes	No
6) Mengganjal ATM	No	Yes	No	No	Yes	No	No	Yes	No	No	No	No	No	Yes
c. Media (Alat)	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1) *Handphone*	No	No	Yes	No	Yes	No	No	No	No	No	No	Yes	No	No
2) Alat Mengganjal Mesin ATM	No	No	No	No	Yes	Yes	No	Yes	No	No	No	No	No	Yes
3) Motor	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No
4) Alat Skimming dan Micro Cam	No	No	No	No	No	No	No	No	No	No	Yes	No	No	No
2. Target (Korban)	No	No	No	No	Yes	No	No	No	No	Yes	No	No	No	No
a. Laki - Laki	No	No	No	No	No	No	No	No	Yes	No	No	No	No	Yes
b. Perempuan	No	No	No	No	No	No	Yes	No	No	No	No	Yes	No	No
3. Place (Tempat)	No	No	No	No	No	No	No	No	No	No	No	No	No	No
a. Offline	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1) Panggilan Telepon	No	No	Yes	No	Yes	No	No	No	No	No	No	Yes	No	No
2) ATM	No	Yes	No	No	Yes	No	Yes	Yes	No	No	No	No	No	Yes
b. Online	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1) Tautan Link	Yes	No	No	No	Yes	No	No	No	Yes	No	No	No	No	No
2) WhatsApp	No	No	No	No	No	No	No	No	Yes	No	No	Yes	Yes	No
B. *Social Engineering Attacks*	No	No	No	No	No	No	No	No	No	No	No	No	No	No
1. Jenis Serangan	No	No	No	No	No	No	No	No	No	No	No	No	No	No
a. *Phising*	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No	Yes	No
b. *Skimming*	No	No	No	No	Yes	Yes	Yes	No	No	No	Yes	No	No	Yes
2. Ancaman Serangan	No	No	No	No	No	No	No	No	No	No	No	No	No	No
a. Kerugian Keuangan	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
b. Pencurian Identitas	No	No	Yes	No	Yes	No	No	No	No	No	Yes	No	No	No
3. Informasi Incaran Pelaku	No	No	No	No	No	No	No	No	No	No	No	No	No	No
a. Data Pribadi Nasabah	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No	Yes	No
b. OTP	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No

Sumber : Diolah Peneliti Menggunakan NVivo 12

Gambar IV. 8 dan Tabel IV.1 merupakan informasi *coding* mengenai gambaran permasalahan penipuan *social engineering* yang dihasilkan saat mengolah hasil data *NCapture* website bank resmi yang telah peneliti olah menggunakan bantuan software *NVivo 12.* Lebih lanjut, dalam *coding* memberikan keterangan "yes" yang artinya saling berhubungan, sedangkan "no" mengartikan tidak saling berhubungan antara poin – poin dari gambaran permasalahan penipuan *social engineering*. Adapun hasil *coding* yang telah peneliti temukan, akan dipaparkan dalam deskripsi penjelasan hasil. Agar dapat mempermudah penjelasan hasil analisis gambaran permasalahan penipuan *social engineering*, peneliti membagi penjelasan tersebut ke dalam 2 (dua) bagian.

Pertama, terkait dengan gambaran permasalahan penipuan *social engineering* pada nasabah bank yang dihubungkan dengan teori *crime triangle*. Pembahasan ini melibatkan tiga unsur yaitu *offender* (pelaku), *target* (korban), *place* (tempat) untuk menggambarkan bagaimana permasalahan penipuan *social engineering* dapat terjadi pada nasabah bank. *Kedua*, terkait dengan serangan *social engineering*, yang menjelaskan mengenai jenis serangan yang sering terjadi, ancaman serangan, serta informasi rahasia incaran pelaku penipuan. Berdasarkan peta analisa diatas mengenai gambaran permasalahan penipuan *social enggineering* pada nasabah bank di Indonesia,maka peneliti akan menjelaskan hasil analisis ke dalam uraian berikut ini :

4.3.1 *Crime Triangle*

1. *Offender* (Pelaku)

Pelaku penipuan *social engineering* merupakan individu atau kelompok yang memiliki niat untuk menipu dengan serangkaian kebohongan atau tipu muslihat dengan cara memanipulasi seseorang secara tidak sadar yang dapat menyebabkan kerugian bagi seseorang seperti kerugian data rahasia, keuangan, pencurian identitas, dan lain – lain.

Serangan *social engineering* dapat ditemukan dilingkungan sekitar seperti link palsu, notifikasi aplikasi palsu, dan file – file yang pernah di download.

Pada hasil penelitian, peneliti mengklasifikasikan *offender* (pelaku) berdasarkan karakteristik, modus, dan media (alat) yang digunakan pelaku saat melakukan kejahatan *social engineering*.

a. Karakteristik Pelaku

Klasifikasi pelaku *social engineering* berdasarkan karakteristik dapat berupa perorangan atau kelompok. Pelaku *social engineering* perorangan cenderung melakukan aksi nya sendiri tanpa bantuan dari orang lain. Sedangkan, pelaku *social engineering* yang berkelompok merupakan sekumpulan individu yang tergabung yang memiliki tujuan untuk melakukan aksi penipuan. Hal ini menandakan bahwa pelaku *social engineering* secara berkelompok lebih banyak bekerja sama untuk membagi tugas agar melakukan aksi kejahatan nya semakin mudah. Sedangkan pelaku penipuan *social engineering* perorangan melakukan aksi kejahatan nya sendiri tanpa ada bantuan orang lain, sehingga untuk melakukan aksinya terdapat keterbatasan kemampuan yang disebabkan melakukan aksi kejahatan hanya sendiri.

Berdasarkan data lapangan pelaku penipuan *social engineering* per orangan atau kelompok dapat melakukan aksi nya secara offline atau online. Pelaku penipuan perorangan cenderung menggunakan panggilan telepon sebagai media offline dan menggunakan situs whatsapp sebagai media online. Hal tersebut dapat dilihat dari kasus penangkapan pelaku penipuan warga Palembang yang telah menguras uang nasabah bank asal Trenggalek hingga Rp 84 juta. Awalnya korban mendapat telfon dari pelaku yang mengaku sebagai petugas bank dan berpura – pura sebagai *call center* bank yang akan menawarkan bantuan kepada nasabah. Setelah itu, pelaku mengalihkan komunikasi melalui *whatsapp* dengan tujuan untuk mendapatkan informasi pribadi calon korbannya.

Masih dengan pelaku perorangan kasus serupa juga terjadi di Provinsi Aceh yaitu penipuan online kepada nasabah bank. Kasus penipuan di Aceh, pelaku melakukan modus operandi dengan mengaku sebagai petugas Bank, pelaku menggunakan panggilan telepon sebagai media *offline* untuk menawarkan penukaran hadiah kepada nasabah. Hal ini diungkapkan oleh Kabid Humas Polda Aceh Kombes Pol. Winardy, S. H., S.I.K.,M. Si dalam siaran pers nya :

"Pelaku melakukan modus operandi kejahatan dengan cara dihubungi oleh oknum yang mengaku petugas bank…."(Kombes Pol. Winardy, 2022)

Dalam kasus yang serupa, pelaku *social engineering* secara berkelompok juga menggunakan cara tersebut yaitu menelfon nasabah dan menyamar sebagai petugas bank, kemudian para pelaku menanyakan data pribadi nasabah. Namun perbedaan nya, pelaku *social engineering* secara berkelompok memiliki peran masing – masing. Seperti kasus penangkapan pelaku penipuan yang terjadi di Jogja. Pelaku LG menyamar sebagai petugas bank saat menelfon korban nya. Kemudian pelaku menanyakan data pribadi nasabah dengan alasan menawarkan perubahan fitur pada aplikasi.

Dalam kasus ini pelaku LG bekerja secara berkelompok. Pelaku LG memiliki peran untuk mentrasfer kembali uang korban ke beberapa rekening yang sudah dipersiapkan dan pelaku LG juga memiliki tugas melakukan pemotongan atas *fee* yang diterima dari dua tersangka lainnya yang masih dilakukan pengejaran.

Namun pelaku *social engineering* secara berkelompok lebih banyak menjalankan aksi kejahatan nya secara offline yaitu di ATM. Berdasarkan data yang di dapat, komplotan penipu *social engineering* telah menyusun rencana dengan membagi tugas masing – masing anggota.

Sama hal nya dengan kasus yang pernah terjadi di Sidoarjo, komplotan pelaku penipuan melakukan aksi nya dengan mengganjal mesin ATM. Menurut Wakasat

Reskrim Polresta Sidoarjo AKP Imam Yuwono, para pelaku ganjal ATM melakukan aksinya berkelompok dengan membagi tugas. Satu orang pura – pura membantu, lainnya mengamati korban saat transaksi.

Kasus serupa juga terjadi di Jepara, Jawa Tengah pada 19 Desember 2021. Tiga pelaku melakukan pembobolan dan pengganjalan mesin ATM menggunakan tusuk gigi. Kapolres Jepara AKBP Warsono, terdapat 3 dari empat pelaku yang ditangkap yaitu EM (40 tahun) asal Tanggerang, Banten, JN (42) asal Pesawaran, Lampung, dan FZ (39) asal Tanggamus, Lampung. Satu lagi tersangka masih dalam proses pencarian petugas.

Para pelaku *social engineering* secara berkelompok tentunya memiliki pembagian tugas masing – masing. Dalam kasus ini ada yang menawarkan bantuan kepada korban, dan dua pelaku lainnya mengintip nomor pin yang dimasukkan oleh korban. Hal ini sesuai dengan konfersi pers Kapolres Jepara AKBP Warsono :

> "Namun, kartu ATM korban sulit dimasukkan ke mesin ATM. Lantas datang tersangka EM yang mencoba membantu korban dengan cara ATM milik tersangka dimasukkan ke mesin ATM dan berhasil. Kemudian dikeluarkan kembali dna mengatakan kepada korban bahwa tidak ada masalah. Selanjutnya, tersangka meminta korban mencoba dengan kartu ATM yang sudah ditukar dengan milik tersangka. Kemudian tersangka menyuruh korban memasukkan nomor pin dan pada saat yang bersamaan tersangka JN dan FZ mengintip nomor pin yang dimasukkan korban." (AKBP Warsono, 2021)

Selain itu, masih dengan kasus yang serupa yaitu komplotan pembobolan ATM dan pemalsuan data nasabah. Terjadi penangkapan tujuh orang tersangka yang berhasil diamankan oleh Polda Bengkulu. Berdasarkan konfersi pers Direktur Ditreskrimum Polda Bengkulu, komplotan pembobolan ATM dan pemalsuan data nasabah ini tersebar di beberapa daerah di Indonesia, tidak hanya di Bengkulu.

> "Untuk keseluruhan komplotan pembobolan ATM dan pemalsuan data nasabah bank yang berhasil diringkus sebanyak sebelas orang dan itu ada yang diamankan di luar Bengkulu," (Kombes Pol Teddy Suhendyawan Syarif, 2022)

Kombes Pol Teddy Suhendyawan juga menyebutkan tujuh orang tersangka diamankan Polda Bengkulu, sedangkan pelaku yang lainnya diamankan oleh pihak kepolisian Kota Semarang dan Kepolisian Kota Binjai. Pelaku berinsial KH, AG, dan WI diamankan pihak Kepolisian Kota Semarang, sedangkan satu tersangka lainnya yaitu CH diamankan pihak Kepolisian Kota Binjai.

Pelaku penipuan secara berkelompok tentunya tiap pelaku telah membagi tugas saat melakukan aksinya. Sama seperti kasus komplotan pembobolan rekening yang terjadi pada Sumatera Selatan. Para pelaku ditangkap oleh Polda Metro Jaya di sebuah gubuk tengah hutan di OKI Sumatera Selatan. Hal ini disampaikan Kanit 2 Resmob Ditreskrimum Polda Metro Jaya :

"Sindikat ini tersembunyi di Kabupaten OKI Sumatera Selatan. Sindikat ini meresahkan masyarakat karena sudah banyak korbannya," (Komisaris Maulana Mukarom, 2022)

Kasus ini terungkap atas laporan dari korban bahwa adanya sindikat begal rekening dengan akun *whatsapp* yang menggunakan logo Bank dan menawarkan layanan ekslusif untuk nasabah yang terpilih. Kasus ini meilibatkan tiga pelaku, yang memiliki peran masing – masing. Hal ini disampaikan oleh Kanit 2 Resmob Ditreskrimum Polda Metro Jaya melalui konfersi pers nya :

"Sindikat yang terorganisir ini punya peran – peranan, pertama mencari korban atau target, kedua sebagai tim IT, tim data, ketiga, peran nya sebagai money changer," (Komisaris Maulana Mukarom, 2022)

Terdapat kasus lain nya, Awalnya nasabah mengalami kejanggalan terhadap transaksi yang keluar dari rekeningnya. Padahal korban tidak merasa melakukan transaski di rekeningnya. Dari kasus ini, Tim Subdit V Siber Ditreskrimum Polda Metro Jaya menangkapan dua orang tersangka yang berinisial O dan D. Sementara dua DPO lainnya masih dalam pengejaran. Hal ini disampaikan dalam konfersi pers nya :

"….Kejanggalan pun terjadi karena nasabah merasa tidak pernah melakukan transaksi di rekeningnya yang dikuasai para tersangka," ," (Kombes Pol Yusri Yunus, 2021)

"Dua orang DPO lagi masih kami kejar. Kami juga masih koordinasi dengan pihak BTPN untuk cari kemungkinan korban lain," (Kombes Pol Yusri Yunus, 2021)

Selanjutnya terdapat kasus yang lain, yang berbeda dengan sebelumnya. Kasus ini termasuk kasus *skimming* yang terjadi di Kota Manado pada Januari tahun 2022. Kasus ini melibatkan beberapa pelaku yang menjadi tersangka yaitu dua pria warga negara Bulagaria yang berinisial MIS alias AM, dan VAK, serta ditemani oleh dua wanita warga negara Indonesia yang berinisial CW, dan ALS. Para pelaku bekerja sama untuk melakukan aksi *skimming* di 26 lokasi mesin ATM Bank SulitGo di wilayah Manado yang sering dilewati. Hal ini ditandai dengan ditemukan alat *skimmer* dalam *card reader* mesin ATM Bank SulutGo. Sebagaimana yang dikatakan oleh Kombes Pol Nasriadi :

"Para pelaku memasang alat skimmer pada mesin – mesin ATM Bank SulutGo yang banyak atau tinggi transaksi perbankannya. Kemudian saat beraksi, sindikat ini terbagi dalam tiga kelompok. Kelompok pertama bertugas memasang alat *skimmer*, kelompok kedua adalah yang datang untuk mengambil atau bertransaksi memakai kartu putih, sedangkan kelompok ketiga adalah eksekutor yang mengambil uang secara cash dan mentransfer ke rekening lain," (Kombes Pol Nasriadi, 2022)

Lebih lanjut, segala aksi *skimming* yang dilakukan oleh para pelaku yang berwarga negara Bulgaria dibantu oleh dua wanita yang berasal dari Indonesia, sehingga masih banyak para pelaku yang terlibat dalam kasus ini. Selain itu terdapat pula para pelaku yang masih dalam tahap pencarianm daftar pencarian yang sebagaimana diungkapkan oleh Kombes Pol Nasriadi :

"Masih ada pelaku lain yang masuk DPO (Daftar Pencarian Orang). Kita telah mengirimkan bukti permohonan cekal ke pihak imigrasi dan juga akan mengirimkan *red notice* ke Divhubinter Polri," (Kombes Pol Nasriadi, 2022)

b. Modus Pelaku

Dalam menjalankan aksinya, pelaku penipuan *social engineering* memiliki cara khusus untuk menjalankan rencana kejahatan nya atau disebut sebagai modus operandi.

Berdasarkan hasil temuan dari lapangan, modus pelaku terdiri dari berbagai macam, berikut diantaranya :

1) Mengaku Sebagai Karyawan Bank

Penyamaran sebagi karyawan Bank merupakan modus pelaku penipuan yang sering dijumpai. Cara ini dilakukan oleh pelaku untuk meningkatkan rasa percaya nasabah ketika pelaku melakukan bujuk rayu kepada korban. Teknik seperti ini dikenal sebagai penipuan *social engineering*, yang kasus ini pernah terjadi pada warga Sleman yang mengakibatkan tabungan nya hilangan Rp 510 juta.

Lebih lanjut, setelah membujuk rayu korban, pelaku menanyakan sejumlah data pribadi korban dengan alasan membantu korban untuk menutup aplikasi berbayar. Kemudian pelaku mengarahkan korban untuk mengirimkan kode aktivasi kepada pelaku, sehingga pelaku dapat mengakses rekening korban.

Teknologi yang semakin berkembang dengan adanya telepon seluler dimanfaatkan pelaku untuk melakukan aksi kejahatan nya. Kasus serupa juga terjadi pada salah satu nasabah bank di Indonesia. Dalam keterangannya di konfersi pers Kabid Humas Polda Metro Jaya Kombes Yusri Yunus , pelaku melakukan panggilan kepada korban dan mengaku sebagai staf Bank. Lebih lanjut, korban pun terpangaruh kepada pelaku yang kemudian mengikuti arahan dari pelaku, sesuai dengan konfersi pers Kombes Yusri Yunus :

"Korban yang terpengaruh kemudian mengikuti petunjuk terduga pelaku dengan mengirimkan login terdaftar dengan mengisi data nasabah dan OTP. Setelah pelaku mendapat akun nasabah, pelaku mengambil alih rekening nasabah kemudian dikuras habis," (Kombes Yusri Yunus,2021)

Kasus serupa juga terjadi di Propinsi Aceh. Perkembangan internet memang semakin berkembang sehingga penipuan online merebak di masyarakat. Kasus ini terjadi pada nasabah bank yang menjadi bujuk rayu pelaku yang menyamar sebagai petugas

bank. Berdasarkan siaran persnya, Kabid Humas Polda Aceh Kombes Pol. Winardy, mengatakan bahwa pelaku melakukan modus operandi mengaku sebagai petugas bank, dan kemudian pelaku menawarkan poin hadiah, yang pada akhirnya pelaku meminta nasabah untuk melengkapi identitasnya.

Adapun kasus lainnya dengan modus pelaku menyamar sebagi petugas bank juga terjadi pada nasabah bank asal Trenggalek. Dalam kasus ini korban dan pelaku tidak berada dalam kota yang sama. Walaupun demikian, pelaku memiliki cara yang cerdik untuk menglabui korban nya. Dalam konfersi persnya, Iptu Agus Salim mengatakan tersangka merupakan warga Palembang, sedangkan korban nya merupakan nasabah bank asal Trenggalek. Konfersi pers ini dilihat berdasarkan hasil penangkapan pelaku yang berhasil diringkus oleh anggota polisi di Palembang.

"Tersangka kami tangkap di Palembang, dengan kerja sama Polda Sumatera Selatan dan Polres setempat," (Iptu Agus Salim, 2022)

Kasus penipuan ini bermula saat korban mendapat telepon dari seseorang yang mengaku sebagai *call center* bank yang meminta sejumlah data nasabah. Hal ini disampaikan oleh Iptu Agus Salim dalam pers nya :

"….. pelaku ini berpura – pura menjadi petugas *call center*. Karena korban dalam kondisi kebingungan akhirnya dengan mudah pelaku memperdayainya," (Iptu Agus Salim, 2022)

Merasa ada yang tidak beres, korban berniat menelpon nomor layanan salah satu bank di Trenggalek di mesin pencarian google. Tapi nomor yang didapati korban adalah nomor palsu yang bukan nomor resmi bank, karena pelaku telah menggantinya nomor *call center* resmi dengan nomor telepon pribadi pelaku.

"Korban mencari tahu melalui mesin pencarian google, dari situlah muncul sebuah nomor telepon pada alamat BRI Unit Kota. Ternayata, nomor itu sudah diubah oleh pelaku menjadi nomor pribadinya," (Iptu Agus Salim, 2022)

Lebih lanjut, pelaku AC mengakui perbuatan nya. Pelaku sengaja mengubah nomor telepon pada rekomendasi alamat bank yang tercantum di google untuk aksi penipuan nya.

"Nomor teleponnya itu kan bisa diubah oleh siapa saja dan saya lihat juga banyak yang sudah diubah. Kemudian saya ubah nomor itu di pertengahan Februari," (AC, 2022)

2) Menawarkan Penukaran Hadiah atau Keuntungan Yang Tidak Wajar

Modus lain yang dilakukan oleh pelaku yaitu menawarkan segala keuntungan untuk menarik perhatian nasabah. Pelaku mengandalkan celah tertentu ketika berkomunikasi dengan calon korban nya, sehingga pelaku menggunakan teknik penipuan *social engineering* untuk membujuk rayu nasabah diiringi dengan tawaran – tawaran yang menarik. Hal ini disampaikan oleh pengamat IT Ruby Alamsyah :

"Teknik yang biasanya dilakukan adalah pendekatan dadakan, yang membuat panik ataupun memberikan informasi kebahagiaan seperti menang undian. Sebagian masyarakat memang tidak langsung percaya, tapi sebagian kecil ada yang percaya. Teknik mereka tadi tinggal dilakukan secara masif," (Ruby Alamsyah, 2020).

Modus yang dilakukan oleh pelaku dengan menawarkan hadiah kepada korban nya merupakan salah satu cara pelaku untuk memancing korban agar mau mengisi data nasabah. Tujuan pelaku adalah mengetahui data nasabah, yang selanjutnya akan digunakan pelaku untuk aksi kejahatan. Hal ini sesuai dengan siaran persnya Kabid Humas Polda Aceh Kombes Pol. Winardy yang mengatakan bahwa :

"Pelaku melakukan modus operandi kejahatannya dengan cara dihubungi oleh oknum yang mengaku petugas bank, kemudian menawarkan penukaran poin hadiah, bantuan untuk melengkapi data nasabah," (Kombes Pol. Winardy, 2022)

Selain itu, terdapat kasus lain seorang dokter yang menjadi korban penipuan nya dengan modus menawarkan keuntungan yang tidak wajar kepada nasabah. Berawal dari seorang dokter mendapat telfon melalui aplikasi whatsapp dari nomor yang tidak dikenal

yang mengaku dari bank pusat. Kemudian, pelaku memberikan tawaran biaya transfer yang lebih murah dibandingkan sebelumnya. Berikut keterangan dari korban :

"Awalnya saya mendapat telepon dari seseorang yang tidak saya kenal dengan nomor +1****** mengaku dari Bank pusat menawarkan perubahan biaya transaksi transfer dari Rp. 6.500 per transaksi menjadi Rp. 150.000 per bulan dan saya bilang tidak mau per bulan, tapi tetap saja ngejar terus," (dr. Binsar, 2022)

Berdasarkan keterangan korban, pelaku berupaya supaya korban tertarik dengan tawaran pelaku, sehingga pelaku terus memaksakan korban menawarkan biaya transaksi transfer tersebut. Setelah itu, pelaku mengirimkan sebuah link kepada korban untuk melengkapi data nasabah terlebih dahulu. Tanpa disadari, korban mengisi data tersebut dan mengirim kembali ke pelaku. Berikut keterangan dari korban :

"Setelah selesai telepon selanjutnya pelaku kirim pesan via WA dan mengirimkan sebuah link. Dari link itulah saya buka dan kembali dikirim ke pelaku." (dr. Binsar, 2022)

Selanjutnya, dari kejadian tersebut tidak berapa lama, korban mendapat notifikasi transaksi di SMS banking bahwa terjadi penarikan uang berkali – kali hingga total 9 transaksi transfer. Kemudian korban pun tersadar bahwa korban telah ditipu dan kehilangan uang di rekening nya.

"Saya sadar saya telah ditipu dan langsung saya telepon *call center* dan saya sudah bilang ada empat ATM saya yang harus saya blokir karena baru sadar saya telah ditipu," ." (dr. Binsar, 2022)

3) Menginfokan Perarturan Baru

Pelaku menggunakan banyak alasan untuk menarik perhatian korban, salah satunya adalah memberikan informasi terkait dengan perarturan baru yang diterbitkan oleh Bank, karena bagi nasabah informasi seperti ini penting dan jika tidak dijalankan maka nasabah akan tertinggal informasi atau mengalami kerugian jika tidak mengikutinya.

Seperti pada kasus penipuan pada warga sleman, yang modus pelaku adalah menawarkan perubahan fitur pada aplikasi yang berbayar, karena merasa keberatan

korban ingin menutup aplikasi tersebut. Kemudian pelaku pura – pura membantu nasabah untuk menutup aplikasi tersebut. Sebelumnya pelaku mengarahkan korban untuk memberi tahu kode aktivasi aplikasi tersebut. Tapi, korban saat itu belum mengetahui kalau dirinya tertipu, jadi korban mengikuti arahan dari pelaku. AKBP Roberto Gomgom Manorang Pasaribu selaku Dirreskrimsus Polda DIY membenarkan hal tersebut, dan beliau juga mengatakan bahwa nomor telepon yang digunakan pelaku bukan yang menggunakan kode khusus yang sering dipakai oleh pihak perbankan.

"Dengan nomor telfon depannya +1. Jadi bukan +62, atau menggunakan kode yang biasa dipakai oleh pihak perbankan," (AKBP Roberto Gomgom Manorang Pasaribu, 2021)

Kontak *call center* tiap bank memiliki kekhususan tersendiri. Hal ini disampaikan oleh Executive Vice President Centre of Digital BCA, Wani Sabu.

"Kalau BCA 1500888, tanpa ada kode area. Kasus ini ditelfon dari angka +1, sudah pasti bukan dari BCA. Bank juga tidak pernah menelfon nasabah untuk diminta data dan suruh ini suruh itu," (Wani Sabu, 2021)

Selesai dari kasus diatas, terdapat kasus lainnya yaitu penipuan terhadap pasangan suami istri di Kota Padang. Awal cerita, korban mendapatkan chat WA tentang pemberitahuan berupa perubahan biaya transfer. Setelah itu, pelaku mengirimkan berupa formulir dan link yang mengarahkan korban untuk mengisinya. Lalu, korban mengikuti arahan tersebut tanpa curiga dengan meng-klik link tersebut dan mendaftarkan username, password, dan pin.

Selanjutnya korban mendapatkan sms dari pihak BRI berupa kode OTP dan link, yang kemudian link tersebut diberikan ke pelaku. Setelah itu, pelaku mendapatkan notifikasi dari aplikasi kalau terdapat transaksi keluar dan uang korban pun hilang. Kasus ini sudah masuk ke laporan Polda Sumbar, sesuai dengan konfersi yang disampaikan oleh Kepala Bidang Hubungan Masyarakat Polda Sumbar Kombes Pol Stefanus Satake Bayu

:

"Saat ini kasus sedang ditangani Direktorat Reserse Kriminal Khusus Polda Sumbar," (Kombes Pol Stefanus Satake Bayu, 2022)

Pelaku penipuan memiliki banyak strategi untuk menjebak korban nya. Modus pelaku dengan memberikan info adanya perarturan baru dari Bank juga dirasakan oleh pria pensiunan dari sebuah perusahaan migas raksasa. Bermula korban mendapat telepon yang mengatasnamakan Bank. Pelaku menjelaskan terdapat perarturan baru tentang biaya transfer yang akan dikenakan Rp. 150.000 per bulan. Saat itu pelaku menawarkan kepada korban beberapa pilihan, jika korban ingin biaya transfer tetap Rp. 6.500 diharuskan untuk mengisi formulir. Lalu, korban mengikuti arahan pelaku dan tidak lama kemudian korban Mz mendapatkan notifikasi dari *smartphone* nya terdapat traksaksi keluar dari rekeningnya, dan uangnya raib dengan tiba - tiba . Hal ini disampaikan oleh korban saat diwawancara :

"Tapi kalau mau biayanya hanya Rp. 6.500 saya disuruh isi form. Salahnya saya form itu, dan disuruh ngisi pilih biaya transfer, terus minta kode aktivasi dan PIN BSI mobile. Dan saya nurut aja waktu itu, " (Mz, 2022)

4) Menawarkan Bantuan

Modus lainnya yang dapat menarik perhatian nasabah adalah dengan menawarkan bantuan kepada nasabah. Pemberikan bantuan kepada nasabah dapat membuat yakin nasabah dengan pelaku, karena pelaku memberikan sikap baik kepada nasabah untuk menolong, sehingga nasabah menganggap pelaku merupakan petugas resmi bank, namun pada kenyataan nya tidak. Itu hanyalah modus semata yang dijalankan oleh pelaku.

Modus dengan menawarkan bantuan pernah dirasakan oleh Ketua KPU Sidaoarjo yang menjadi korban. Awal kasus ini terjadi ketika, Ketua KPU Sidoarjo Muhammad Iskak mengambil uang di mesin ATM di salah satu Kawasan perumahan. Ketika memasukkan kartu, namun gagal berkali – kali. Kemudian korban keluar ATM dan

bertemu dengan orang yang tidak dikenal yang sepertinya sudah mengintai korban saat memasukkan kartu ATM. Berikut penjelasan dari Ketua KPU Sidoarjo selaku korban :

"Karena tidak bisa saya lalu keluar ATM. Di luar ada orang yang tidak saya kenal tawarkan bantuan. Kartu saya bisa masuk tapi tak dapat transaksi hanya terdengar suara di mesin. Saya cancel dan cabut kembali kartunya tapi seperti tersangkut," (Muhammad Iskak, 2021)

"Sudah saya laporkan. Mereka memang sepertinya sudah mengintai sejak saya masuk ATM." (Muhammad Iskak, 2021)

Setelah mengetahui ATM nya bermasalah, korban lalu meninggalkan tempat tersebut dan menuju ke kantor cabang bank terdekat. Dalam perjalanan, korban terkejut setelah mendapat sms notifikasi proses transfer berhasil. Setelah dicek, ternyata tabungan nya dikuras habis oleh pelaku. Modus pelaku yang dilakukan dalam kasus ini, adalah menukar kartu ATM korban dengan pelaku. Sebagaimana yang disampaikan oleh Wakasat Reskrim Polresta Sidoarjo :

"Kami masih selidiki. Jadi uang itu ada yang diambil tunai dan ditransfer. Modusnya dengan menukar kartu ATM korban dengan pelaku. Untuk nomor pin sudah mereka ketahui saat korban memasukkan kartu ATMnya" (AKP Imam Yuwono)

Selain kasus di atas, terdapat kasus lain nya yang menggunakan modus menawarkan bantuan. Kasus yang akan dibahas berikut ini, serupa dengan kasus diatas. Pada kasus ini, pelaku telah mengganjal mesin ATM sebelum korban menggunakan nya. Korban yang bernama Saekul saat itu hendak mengambil uang melalui mesin ATM di sebuah SPBU. Namun saat kartu dimasukkan ke mesin ATM, kartu tersebut sulit untuk masuk. Kemudian pelaku EM saat itu posisinya di ATM dan menawarkan bantuan ke korban, dengan cara pelaku memasukkan kartu ATM miliknya ke mesin ATM dan berhasil. Setelah itu pelaku mengatakan kepada korban bahwa mesin ATM tersebut tidak bermasalah. Hal ini disampaikan oleh Kapolres Jepara :

"Namun, kartu ATM korban sulit masuk ke mesin ATM. Lantas datang tersangka EM yang mencoba membantu korban dengan cara ATM milik tersangka dimasukkan ke

mesin ATM dan berhasil. Kemudian dikeluarkan kembali dan mengatakan kepada korban bahwa tidak ada masalah," (AKBP Warsono, 2022)

Selanjutnya pelaku meminta korban mencoba kembali dengan kartu ATM yang sudah ditukar dengan milik tersangka. Kemudian pelaku menyuruh teman nya untuk mengintip nomor pin saat kartu dimasukkan oleh korban. Berikut penjelasan Kapolres Jepara :

"Kemudian tersangka menyuruh korban memasukkan nomor pin dan pada saat yang bersamaan tersangka JN dan FZ mengintip nomor pin yang dimasukkan korban." (AKBP Warsono, 2022)

Selain itu terdapat kasus yang lain, kasus berikut ini pelaku memberikan tawaran bantuan untuk menutup aplikasi M-Banking karena aplikasi M-Banking miliki korban PS sedang dalam perbaikan, sehingga korban diminta biaya senilai Rp. 300.000 sejumlah tiga rekering milik korban. Hal ini disampaikan oleh Direktur Kriminal Khusus Polda DIY :

"Pelaku ini memberitahu PS bahwa aplikasi M-Banking ada perbaikan pada fiturnya dan meminta biaya perbaikan dan top up," (AKBP Roberto Gomgom Manorang, 2021)

Setelah pelaku memberikan tawaran bantuan kepada korban, pelaku menyuruh korban untuk menyebutkan PIN OTP milik korban. AKBP Roberto Gomgom Manorang mengatakan :

"Tiba – tiba muncul sms ada one time password (OTP). OTP adalah kode akses yang dimiliki pada aplikasi dimana aplikasi itu bisa diakses atau tidak berdasarkan kode otoritas," (AKBP Roberto Gomgom Manorang, 2021)

Setelah dibujuk oleh pelaku sebanyak tiga kali, korban pun menyebutkan pin tersebut, karena posisi korban saat itu sedang panik dan sedang mengantar keluarga ke rumah sakit. Ketika telah mengetahui PIN OTP tersebut, pelaku langsung mencuri uang di rekening korban. Berikut penjelasan dari AKBP Roberto Gomgom Manorang :

"Tak lama berselang korban mendapatkan pemberitahuan melalui sms bahwa transaksi berhasil. Pelaku sudah mengetahui kelemahan korban karena sudah mengirimkan OTP," (AKBP Roberto Gomgom Manorang, 2021)

5) Permintaan Mengisi Data Nasabah

Berbagai modus yang dilakukan oleh pelaku, pada akhirnya tujuan pelaku adalah mendapatkan data pribadi nasabah yang nantinya akan digunakan untuk aksi kejahatan nya. Hasil dari lapangan menunjukkan bahwa setelah pelaku menawarkan bantuan atau hadiah, pelaku mengarahkan korban untuk mengisi data nasabah terlebih dahulu agar bantuan atau hadiah dapat diproses atau diberikan. Berdasarkan hasil dari lapangan, pelaku menggunakan link sebagai perantara nasabah untuk mengisi identitasnya. Penggunaan link ini membuat perbuatan pelaku seolah – olah resmi dari Bank, sehingga membuat percaya nasabah.

Modus pelaku yang meminta nasabah untuk mengisi data nya terjadi di Propinsi Aceh. Dalam kasus ini, pelaku menelfon korban nya dengan berpura – pura menjadi petugas bank, dan menawarkan hadiah. Namun, sebelum nasabah menukarkan hadiahnya, nasabah terlebih dahulu diperintahkan untuk melengkapi data pribadi nasabah seperti kode OTP, PIN, dan Password melalui link yang dikirim pelaku. Hal ini diungkapkan oleh Kabid Humas Polda Aceh Kombes Pol. Winardy, S. H., S.I.K.,M. Si dalam siaran pers nya :

"…. Modusnya adalah pengiriman link untuk permintaan data nasabah. Setelah itu, pelaku melakukan permintaan OTP/kode aktivasi mobile banking."(Kombes Pol. Winardy, 2022)

Ketika pelaku telah mendapatkan data nasabah, selanjutnya pelaku menggunakan data tersebut untuk mengambil uang nasabah di rekening. Sama hal nya dengan kasus yang lain yaitu pengungkapan kasus pengambilalihan rekening salah satu bank. Modus yang dilakukan pelaku terbilang rapih. Berawal pelaku mengaku sebagai petugas bank, kemudian pelaku berhasil menyakinkan korban untuk mengisi link web, sehingga pelaku

berhasil mengusai identitas dan akun nasabah. Berikut pernyataan dari Kabid Humas Polda Metro Jaya :

"Korban yang terpengaruh kemudian mengikuti petunjuk pelaku dengan mengirimkan login terdaftar dengan mengisi data nasabah dan OTP. Setelah pelaku mendapat akun nasabah, pelaku mengambil rekening nasabah kemudian dikuras habis," (Kombes Pol Yusri Yunus, 2021)

Selain itu, terdapat kasus lainnya dengan modus pelaku meminta data nasabah. Kasus penipuan yang dialami oleh korban berinisial E yang merupakan karyawan di perusahaan swasta di Jakarta. Pada awalnya korban E melakukan transaksi pembelian pulsa di mobile banking dan selalu gagal. Lalu, korban E mencoba untuk menghubungi salah satu bank di Indonesia melalui social media. Kemudian, tidak lama dari kejadian tersebut, pelaku mengirimkan DM kepada korban dengan memakai akun yang mirip akun sosial media miliki Bank resmi. Korban pun terkecoh dengan isi DM tersebut, karena pelaku mengaku sebagai CS bank.

Kemudian, pelaku berdalih akan melakukan refund sehingga pelaku mendesak korban E membuka sebuah link untuk mengisi form data diri, agar refund bisa segera di proses. Berikut pernyataan dari korban E :

"Dia (penipu) suruh saya isi data diri tersebut. Pas ditanyain alasannya macam – macam. Saya tidak balas malah diteror terus sama nomor tersebut,". (E, 2021)

Selanjutnya, terjadi juga kasus dengan modus seperti ini di Padang. Kasus seorang nasabah salah bank di Indonesia menjadi korban siber dengan link phising. Kasus ini sudah ditangani oleh Polresta Padang, dan penyidik sudah mengumpulkan keterangan saksi dan barang – barang bukti yang terdapat di TKP. Hal ini disampaikan oleh Kasat Reskrim Polresta Padang :

"Kita juga sudah minta keterangan saksi dari korban itu sendiri guna penyelidikan yang lebih lanjut," (Kompol Dedy Adriansyah, 2022)

Kasus ini bermula saat korban mendapatkan pesan melalui Whatsapp tentang pemberitahuan berupa perubahan biaya transfer. Lalu, korban dikirimkan oleh pelaku link untuk melengkapi isi formulir. Formulir tersebut yang mengarahkan korban untuk mendaftarkan username, password, dan pin. Saat itu korban mengikuti perintah pelaku untuk mengisinya, sehingga pelaku mudah untuk mencuri uang yang ada di rekening korban.

6) Mengganjal ATM

Modus pelaku mengganjal ATM dengan bantuan alat sudah sering terjadi di ATM sekitar. Alat yang sering digunakan pelaku adalah tusuk gigi, karena bentuknya kecil dan harganya murah, sehingga mudah untuk di dapatkan. Adapun kasus yang terjadi dengan modus seperti ini yaitu penangkapan dua belas kawanan perampok spesialis nasabah bank yang sering beraksi di wilayah Depok hingga Tanggerang Selatan oleh Tim Subdit Resmob Ditreskrimum Polda Metro Jaya. Modus yang dilakukan para pelaku yaitu mengganjal ATM dengan tusuk gigi untuk menahan kartu ATM milik korban supaya tidak dapat masuk ke mesin ATM. Umumnya, setelah para pelaku berhasil melakukan aksi tersebut, mereka membagi tugas, yaitu satu orang berpura – pura membantu korban dengan cara memasukkan kartu ATM milik pelaku yang seolah – seolah berhasil tanpa ada masalah, dan teman – teman pelaku yang lainnya berusaha mengintip PIN yang dimasukkan oleh korban ketika korban mencoba kedua kalinya memasukkan PIN ATM. Pada akhirnya, setelah pelaku mengetahui PIN ATM nasabah, para pelaku segera untuk mengambil uang di rekening nasabah sebelum nasabah tersebut memblokir kartu ATM miliknya.

7) Media (Alat) Yang Digunakan Pelaku

Dalam melakukan kejahatan, tentunya pelaku menggunakan media sebagai perantara untuk melancarkan aksi kejahatan nya. Sama seperti hal nya dengan penipuan *social*

engineering ini, pelaku penipuan menggunakan beberapa alat atau media yang digunakan diantara nya

a) Handphone

Penipuan *social engineering* identik dengan menglabui korban agar mendapatkan informasi pribadi nasabah dengan cara memanipulasi korban dengan cara yang halus. Cara nya dapat dilakukan dengan bujuk rayu kepada nasabah, dengan berpura – pura sebagai petugas bank. Namun untuk melakukan aksi tersebut, pelaku harus menggunakan alat atau media untuk menghubungi korban. Umumnya pelaku menggunakan handphone untuk menghubungi korbannya . Hal ini diungkapkan oleh Dirreskrimsus POLDA DIY :

"Metodenya kita kenal dengan nama *social engineering*, pelaku mencoba melakukan bujuk rayu, menyamar, kemudian menelpon korban," (AKBP Roberto Gomgom Manorang, 2021)

Hal tersebut juga diungkapkan oleh Kasat Reskrim Polres Trenggalek Iptu Agus Salim saat konfersi pers mengenai kasus penangkapan pelaku penipuan yang menyamar sebagai *call center* bank hingga menguras uang nasabah puluhan juta. Ketika komunikasi antar pelaku dan korban berlangsung, pelaku berlagak membimbing korban untuk mengamankan saldo rekeningnya. Hal ini dilakukan agar korban percaya dengan pelaku bahwa pelaku merupakan *call center* resmi bank. Namun kenyataan nya, justru pelaku mengambil uang nasabah di saat nasabah merasa kebingungan. Berikut konfersi pers Kasat Reskrim Polres Trenggalek :

"Saat menerima telepon korban, pelaku ini berpura – pura menjadi petigas *call center*. Karena korban dalam kondisi kebingungan akhirnya dengan mudah pelaku memperdayainya," (Iptu Agus Salim, 2022)

Selain itu terdapat kasus lain nya yaitu penangkapan sindikat penipuan rekening yang beroperasi di Sumatera Selatan. Para pelaku ditangkap di sebuah gubuk tengah hutan di Kawasan Ogan Komering Ilir (OKI). Kasus ini terungkap setelah korban melaporkan adanya pelaku pembegalan rekening dengan menggunakan modus menggunakan logo

Bank dan menawarkan layanan ekslusif bagi nasabah terpilih. Dalam penangkapan ini, penyidik menyita 53 barang bukti, mulai dari merek ponsel, buku tabungan banj, senjata tajam, senjata api, hingga narkoba jenis sabu. Berikut penjelasan dari Kanit 2 Resmob Ditresmum Polda Metro Jaya. :

> "Kita tangkap disitu dan kita temukan juga senjata api rakitan peluru dan ada narkoba juga kita temukan narkoba jenis sabu. Selain mereka sindikat, mereka juga pengedar narkoba. Perkara narkoba nya kami koordinasi dengan Direktorat Narkoba Polda Metro," (Komisaris Maulana Mukarom, 2022)

b) Alat Pengganjal Atm

Alat yang sering digunakan para pelaku penipuan adalah alat yang memiliki harga yang ekonomis dan mudah dimiliki oleh para pelaku. Salah satu contohnya adalah tusuk gigi. Berbekal tusuk gigi, para pelaku dapat melakukan aksi kejahatan nya tanpa mengalami kesulitan.

Contoh kasusnya adalah kasus pengganjal mesin ATM di Jepara dan di Depok. Berawal korban ingin memasukkan kartu ke mesin ATM, namun korban mengalami kesulitan ketika memasukkan nya, karena pelaku telah mengganjal mesin ATM dengan tusuk gigi untuk menahan kartu ATM milik korban yang nantinya kartu ATM tersebut akan ditukar oleh pelaku dengan kartu ATM milik pelaku. Dengan demikian, kartu ATM milik korban yang telah ditukar oleh pelaku akan dimanfaakan oleh pelaku untuk mengambil uang dalam rekening tersebut.

c) Motor

Dalam rangka melancarkan aksi kejahatan nya, pelaku menggunakan kendaraan motor untuk mencapai ke tempat penipuan atau digunakan untuk memburu korban nya. Contohnya adalah kasus penangkapan dua belas kawanan perampok yang mengganjal mesin ATM. Pelaku menggunakan motor tersebut untuk membututi atau memburu korban, setelah korban mengambil uang di bank. Selanjutnya pelaku akan memiliki cara

agar korban berhenti di jalan yaitu membuat ban kendaaran milik korban kempes dengan menggunakan paku. Hal ini disampaikan oleh Kapolda Metro Jaya :

"Selain itu para tersangka juga menyasar korbannya yang selalu membawa kendaraan roda empat usai mengambil uang di bank. Setelah itu pelaku lainnya anggota kawanan ini, akan membututi korban dengan sepeda motor dan membuat kendaraan kempes ban dengan menggunakan paku dilapisi karet," (Irjen. Pol. Drs. Nana Sujana, M.M., 2020)

2. *Target* (Korban)

Korban penipuan *social engineering* di dunia perbankan adalah nasabah Bank yang mengalami manipulasi psikologi yang secara tidak sadar melakukan tindakan yang dapat merugikan nasabah sendiri seperti pencurian data nasabah, dan kerugian keuangan. Penipuan *social engineering* dapat ditemukan dimana saja, jika dilihat di data penipuan *social engineering* banyak di temukan di pulau jawa dibandingkan di pulau lainnya. Dengan demikian area cakupan pelaku penipuan *social engineering* luas, tidak hanya pada satu area saja. Selain itu pelaku penipuan juga dapat beraksi melalui sosial media dilihat dari korban yang bernama mika yang dilabui oleh pelaku yang mengatasnamakan bank melalui Instagram. Hal ini menandakan bahwa pelaku tidak harus bertemu langsung dengan korban nya, namun yang dilakukan oleh pelaku adalah mengetahui kelemahan korban agar dapat terjerumus dalam jebakan nya.

Selain itu, pelaku penipuan memburu korban nya tidak mengenal status pekerjaan nya ataupun tingkat pendidikan nya. Namun pelaku memburu korban yang mudah dibujuk rayu, dan dimanipulasi psikologis nya saat itulah pelaku mengetahui kelemahan korban nya. Hal ini ditujukkan dengan korban yang bernama dr. Binsar Parhusip yang saat itu berprofesi sebagai dokter bedah. Pada saat kejadian dr. Binsar Parhusip sedang sibuk bertugas di rumah sakit, sehingga pelaku memiliki peluang untuk memanipulasi psikologis korban, karena dengan hal tersebut korban tidak sadar bahwa dirinya sedang di bujuk rayu agar masuk perangkap pelaku.

3. *Place* (Tempat)

Place atau tempat diartikan sebagai lokasi terjadinya peristiwa bertemunya *target* (korban) dan *offender* (pelaku). Pada bagian ini, peneliti akan menunjukkan tempat yang menjadi titik temu pelaku dan korban bertemu, yang menyebabkan penipuan *social enginnering* terjadi. Penipuan social enginnering dapat dilakukan secara offline dan online, berikut perincian nya :

a. *Offline*

Penipuan *social engineering* dapat dilakukkan secara *offline,* yang bermakna bahwa aksi penipuan nya tidak menggunakan jaringan internet seperti panggilan telepon dan pertemuan di ATM. Berikut penjelasan nya :

1) Panggilan Telepon

Pada umumnya cara agar pelaku dapat berkomunikasi dengan korban adalah melalui panggilan telepon. Melalui panggilan telepon ini, pelaku mulai memberikan bujuk rayu serta iming - iming hadiah menarik untuk meluluhkan korban. Selanjutnya,pelaku akan mengarahkan korban untuk melengkapi data nya sembari dengan memberikan tipu muslihat oleh pelaku. Sama seperti yang dikatakan oleh Dirreskrimsus Polda DIY saat konfersi pers mengenai kasus penipuan *social engineering* pada warga Sleman :

"Metodenya kita kenal dengan nama *social engineering,* pelaku mencoba melakukan bujuk rayu, menyamar kemudia menelpon korban." (AKBP Roberto Gomgom Manorang Pasaribu, 2021)

Melalui panggilan telepon, umumnya pelaku akan meyakinkan korban bahwa pelaku tidak mencerminkan sebagai penipu. Maka dari itu, pelaku berpura – pura

mengaku sebagai petugas bank atau *call center* bank. Hal ini sesuai yang disampaikan oleh Kabid Humas Polda Metro Jaya saat konfersi pers mengenai kasus pengambilalihan akun bank digital JENIUS :

"Pengungkapan kasus akses illegal terjadi pada 14 nasabah bank berawal dari telepon dari seseorang yang mengaku staf Bank BTPN. Kejanggalan pun terjadi karena nasabah merasa tidak pernah melakukan transaksi di rekeningnya yang dikuasai para tersangka," (Kombes Pol Yusri Yunus, 2021)

Aksi pelaku yang berpura – pura menjadi petugas bank merupakan cara yang ampuh untuk meyakinkan korban agar korban percaya bahwa pelaku merupakan petugas resmi dengan cara memberikan informasi yang berkaitan dengan kartu kredit, atau informasi lainnya yang berkaitan dengan perarturan bank. Salah satu contoh kasusnya adalah korban yang bernama Dicky sebagai salah satu korban yang uangnya raib dicuri pelaku. Dicky mengungkapkan bahwa alasan mempercayai telepon dari pelaku adalah telepon resmi dari bank yang menginformasikan bahwa kartu kreditnya berhasil diblokir dan terdapat satu email konfirmasi masuk yang mengatakan bahwa kartu kredit berhasil diblokir.

Berikut pernyataan Dicky selaku korban :

"Sehingga, saya percaya bahwa mereka dari Bank Mega, apalagi telepon berlangsung tiga kali hampir lebih dari 90 menit totalnya," (Dicky, 2022)

Adapun kasus serupa dari kasus yang lain, yaitu korban yang bernama MZ menjadi korban penipuan akibat dibohongi pelaku yang mengaku sebagai petugas bank melalui panggilan telepon. Modus yang digunakan pelaku saat itu adalah menginformasikan perarturan baru terkait biaya transfer yang naik menjadi Rp. 150.000 per bulan. Adapun opsi lain yang ditawarkan pelaku adalah jika ingin biaya transfer tetap Rp. 6.500, korban di arahkan untuk mengisi form yang dikirim pelaku. Berikut penjelasan dari korban :

"Tapi kalau mau biayanya hanya Rp. 6.500 saya disuruh isi form. Salahnya saya form itu, dan disuruh ngisi pilih biaya transfer…. ," (MZ, 2022)

2) ATM (Anjungan Tunai Mandiri)

Selain melalui panggilan telepon untuk berkomunikasi dengan korban, pelaku juga mengincar korban nya di ATM, sehingga terjadilah pertemuan antara korban dan pelaku. ATM merupakan fasilitas yang disediakan oleh bank untuk memudahkan nasabah dalam bertransaski. Namun, di sisi lain terdapat sisi negatif ketika nasabah bertransaksi di ATM, yaitu maraknya kejahatan yang dapat merugikan nasabah.

Selanjutnya, peneliti akan menerangkan beberapa kasus yang terjadi tentang pelaku yang telah mengincar korbannya di ATM dalam rangka melakukan aksi kejahatan nya :

a) Pembobolan ATM di Cirebon

Bermula korban yang bernama Iin Kristina mengambil uang di ATM pada pagi hari jam 7, pada penarikan pertama sebesar Rp. 1.250.000 kartu atm korban tertelan mesin, dan tidak dapat dikeluarkan, sehingga penarikan uang pun gagal. Hal ini pun disampaikan oleh korban :

"Jam 7 pagi saya berangkat dari rumah, mampir ke ATM Tuparev POM bensin. Baru pengamilan pertama Rp. 1.250.000 kartu ATM saya ketelen," (Iin, 2021)

Setelah menyadari kartu ATM nya tertelan, korban pun langsung mengurus pemblokiran kartu ATM yang tertelan. Namun saat korban menghubungi pihak Bank melalui telepon, korban justru mendapatkan informasi bahwa uang nya telah raib karena pembobolan rekening.

b) Kasus Penarikan Uang Nasabah Yang Berdomisili Bandung

Pada mula nya korban mendapatkan informasi bahwa terjadi penarikan uang dari rekening korban di daerah Surabaya, yang mana bukan tempat tinggal korban. Adapun

penarikan uang terjadi, korban tidak mengetahui. Setelah di identifikasi ternyata penarikan uang tersebut dilakukan di ATM Surabaya, padahal pada saat itu kartu ATM sedang berada ditangan korban. Berikut penjelasan dari korban :

"Tabungan gue diambil 135 juta di jam 1 pagi, 27 Maret 2022 via penarikan ATM. Padahal ini (kartu) atm di gue, gue pegang. Gue domisili di Bandung, tapi penarikan ini dilacak di Surabaya kata CS BCA," (Hebbie, 2022)

c) Ketua KPU Sidoarjo Menjadi Korban Modus Ganjal ATM

Awal cerita korban yang baru slesai pulang dari kantor, mengambil uang di mesin ATM. Namun saat itu korban tidak dapat memasukkan kartunya, karena kartu ATM nya tersangkut. Pada saat kejadian ternyata diluar pintu ATM sudah ada orang yang menawarkan bantuan sekaligus mengintai korban. Berikut informasi dari korban :

"Karena tidak bisa saya lalu keluar ATM. Di luar ada orang yang tidak saya kenal tawarkan bantuan. Kartu saya bisa masuk tapi tak dapat transaksi hanya terdengar suara di mesin. Saya cancel dan cabut kembali kartunya tapi seperti tersangkut," (Muhammad Iskak, 2021)

d) Pengganjal Mesin ATM di Jepara

Pengungkapan kasus ini berawal laporan dari korban yang bernama Saekul yang sebelumnya melakukan penarikan di mesin ATM SPBU di kecamatan Tahunan di Jepara. Saat itu kartu ATM milik korban sulit dimasukkan ke mesin ATM. Kemudian, ketika korban sedang memasukkan kartu, terdapat seseorang yang membantu dari luar. Seseorang ini merupakan pelaku yang telah mengintai korban dari luar yang berpura – pura membantu korban untuk memasukkan kartu. Sekaligus pelaku tersebut yang menukar kartu ATM korban dengan miliknya ketika pelaku menyuruh korban untuk mencoba kembali memasukkan kartu yang sudah di tukar oleh pelaku. Berikut keterangan dari Kapolres Jepara AKBP Warsono :

"Namun, kartu ATM korban sulit masuk ke mesin ATM. Lantas datang tersangka EM yang mencoba membantu korban dengan cara ATM milik tersangka dimasukkan ke mesin ATM dan berhasil. Kemudian dikeluarkan kembali dan mengatakan kepada korban bahwa tidak ada masalah," (AKBP Warsono, 2022)

e) Penangkapan Dua Belas Kawanan Perampok Spesialis Nasabah Bank

Penangkapan dua belas kawanan perampok spesialis nasabah bank ini dilakukan oleh Direktorat Reserse Kriminal Polda Metro Jaya. Hal ini disampaikan melalui konfersi pers yang di pimpin oleh Kapolda Metro Jaya Irjen. Pol. Drs. Nana Sujana, M.M pada tanggal 19 Juni 2020. Dalam penjelasan nya, para perampok ini sering melakukan modus penipuan di mesin ATM , dan telah beraksi di wilayah Depok sampai Tanggerang Selatan hingga sembilan kali . Modus yang dilakukan sama dengan pelaku – pelaku ganjal ATM pada umumnya yaitu mengganjal mesin ATM dengan tusuk gigi supaya dapat menahan kartu ATM milik korban.

f) Penangkapan Komplotan Pembobol ATM dan Pemalsuan Data Nasabah

Penangkapan ini dilakukan oleh Direktorat Reserse Kriminal Umum Polda Bengkulu yang telah menangkap komplotan pembobol ATM yang tersebar dibeberapa daerah di Indonesia. Penangkapan ini telah meringkus sebelas orang tersangka, yang diantaranya tujuh orang tersangka ditangkap di Bengkulu, dan empat lain nya telah diamakan diluar Bengkulu. Hal ini disampaikan oleh Direktur Ditreskrimum Polda Bengkulu :

"Untuk keseluruhan komplotan pembobol ATM dan pemalsuan data nasabaha bank yang berhasil diringkus sebanyak sebelas orang dan itu ada yang diamankan di luar Bengkulu," (Kombes Pol Teddy Suhendyawan Sayrif, 2022)

g) Pembobolan Rekening Nasabah di Kabupaten Bojonegoro

Kasus pembobolan rekening ini dialami oleh korban yang bernama Aris. Kasus pembobolan rekening ini di duga dilakukan dengan cara mencuri data nasabah atau *skimming*. Korban mengaku kehilangan uang nya, dan merasa tidak pernah melakukan transaksi sama sekali sebelumnnya. Korban panik karena ketika di ATM ingin melakukan penarikan uang, saldo korban kurang mecukupi. Padahal sebelumnya saldo korban masih sekitar Rp. 13.000.000. Berikut pernyataan dari korban :

"Kemarin saya mau melakukan transaksi di ATM tetapi saldonya kurang, padahal saldo saya sebelumnya sekitar Rp. 13 jutaan sekian," (Aris, 2021)

h) Dua Rekening Milik Seorang Wanita Dibobol Secara Bersamaan

Berdasarkan cuitan di twitter dari akun korban @nurultryani mengaku bahwa wanita tersebut kehilangan uang di dua rekening dari bank yang berbeda. Berawal dari korban yang pernah melakukan penarikan uang di mesin ATM SPBU di daerah Beji, Depok, dan mesin ATM yang terdapat di Alfa Midi, Beji, Depok. Setelah itu terjadi penarikan uang di jam 4 pagi, yang menurut informasi korban, bahwa korban tidak merasa melakukan transaksi tersebut. Kemudian korban langsung menghubungi *customer service* untuk melakukan pemblokiran. Berikut pernyataan dari korban :

"Dri CS BCA itu bilang kalau penarikan jam 4 pagi. Dari mutasi rekening, ada *switching* kartu di SPBU padahal saya enggak pernah tarik tunai BCA di mesin ATM SPBU," (Nurul Tryani, 2021)

b. Online

Berkembangnya teknologi di Indonesia, membuat serangan penipuan menjadi beragam. Meskipun dengan hadirnya internet memudahkan manusia untuk memperoleh segala jenis informasi. Namun, hal ini juga memberikan kemudahan bagi penipu untuk melancarkan aksi kejahatan nya. Pelaku dapat memanfaatkan jaringan internet ini sebagai

media untuk melakukan kejahatan nya melalui berbagai aplikasi atau fitur yang tersedia secara gratis, seperti penggunaan tautan link, dan whatsapp. Berikut penjelasan nya :

1) Tautan Link

Berdasarkan data lapangan, setelah pelaku melakukan penyamaran sebagai petugas bank dan membujuk rayu nasabah, selanjutnya pelaku akan mengarahkan korban pada sebuah tautan link yang menghubungkan korban dengan sebuah form, atau situs website. Penggunaan link ini telah dirancang oleh pelaku agar memudahkan korban untuk berkomunikasi langsung dengan pelaku. Selain itu, penggunaan tautan link ini bertujuan untuk meningkatkan kepercayaan korban kepada pelaku, karena pemberian tautan link ini di rancang sebagai bentuk modernisasi yang mirip dengan layanan di Bank

Form ini telah dirancang oleh pelaku yang umumnya berisi poin – poin tentang identitas nasabah, pin OTP, Password akun nasabah. Dengan form ini nasabah akan diperintahkan oleh pelaku untuk melengkapi nya. Hal ini sesuai dengan penjelasan oleh Kabid Humas Polda Aceh Kombes Pol Winardy, yang mengatakan bahwa pelaku melakukan modus dengan mengirimkan link untuk permintaan data nasabah, setelah itu pelaku melakukan permintaan OTP/kode aktivasi *mobile banking*.

Setelah pelaku berhasil mendapatkan identitas beserta akun nasabah, selanjutnya pelaku akan mengambil uang dari rekening korban. Hal ini mudah dilakukan karena pelaku telah memiliki akses untuk masuk ke dalam rekening korban. Sebagaimana yang disampaikan oleh Kabid Humas Polda Metro Jaya saat konfersi pers tentang pengungkapan kasus pengambilalihan rekening milik nasabah bank BTPN :

"Jadi saat OTP keluar otomatis data nasabah diambil alih oleh para pelaku dan kuras habis isi rekening empat belas korban," (Kombes Pol Yusri Yunus, 2021)

Selain itu, terdapat juga tautan link yang akan terhubung ke sebuah kontak whatsapp milik pelaku. Tautan link yang menghubungkan ke kontak whatsapp pelaku juga pernah dirasakan oleh korban yang bernama Mika, yang awalnya Mika memberikan aduan atas keluhan nya di salah satu feed akun instagram Bank. Setelah itu Mika mendapatkan pesan dari bank yang memiliki nama dan *profile picture* sama persis dengan akun bank yang terverifikasi. Pesan tersebut berisi sebuah link yang secara otomatis terhubung dengan akun chat milik pelaku. Lewat obrolan pada pesan whatsapp, pelaku menyamar sebagai petugas bank dan menanyakan keluhan Mika. Setelah chatingan lebih jauh, Mika mendapatkan tautan link baru yang mengarahkan korban untuk login di situs website bank buatan pelaku, berikut keterangan dari korban :

> "Dia (penipu) ngarahin untuk login dari link yang baru dikasih. Untungnya, saya sadar kalau alamat situs webnya berbeda dengan website bank yang resmi. Tampilannya juga beda, kayak microsite gitu," (Mika, 2021)

Berdasarkan keterangan dari korban bahwa tampilan situs website yang dibuat oleh pelaku memang berbeda dari situs website bank yang resmi. Pembedanya adalah dari alamat situs website dan tampilannya web pagenya yang dapat dikenali oleh korban. Walaupun pelaku telah membuat situs website dimiripkan dengan situs website bank yang resmi, maka pada ujungnya situs website tersebut dapat dikenali oleh nasabah, bahwa situs website yang dibuat pelaku adalah palsu.

2) Whatsapp

Whatsapp merupakan sebuah platform yang menyediakann layanan bertukar pesan, melakukan panggilan, dan mudah untuk dimiliki karena aplikasi ini gratis dan ditemukan pada berbagai telepon seluruh dunia. Media *whatsapp* digunakan oleh pelaku untuk berkomunikasi dengan korban nya. Interaksi antara korban dan pelaku sering terjadi di whatsapp karena aplikasi whatsapp memiliki fitur yang memudahkan pelaku

untuk mengirimkan gambar, tautan link, video dan lainnya, sehingga aplikasi whatsapp dijadikan sebagai media pendekatan antara pelaku dengan korban.

Cara kerja pelaku ketika menggunakan aplikasi whatsapp tentunya diawali dengan berbagai modus, yang umumnya modus dilakukan pelaku adalah berpura – pura menjadi petugas bank yang ingin membantu korban. Salah satu contohnya adalah kasus penangkapan warga Palembang yang menjadi pelaku penipuan modus *call center* bank. Saat itu kondisi korban sedang mengalami kepanikan karena korban telah menjadi perobaan penipuan dari telepon lain. Kondisi seperti ini pelaku sengaja memanfaatkan kepanikan korban untuk menguras saldo korban yang ada di rekening. Pelaku berinisial AC yang saat itu mengaku sebagai call center berlagak membimbing korban untuk mengamankan saldo rekening. Namun kenyataannya, pelaku justru mengarahkan korban untuk mentransfer uang yang ada dalam rekening ke dalam dompet digital melalui virtual account. Pelaku saat itu menggunakan aplikasi whatsapp sebagai media komunikasi antar pelaku dengan korban. Berikut keterangan dari pelaku AC :

"Kemudian saya bilang, sini saya bantu supaya tidak bisa diakses oleh orang lain. Kemudian saya alihkan ke whatsapp dan saya minta untuk mengirimkan kode untuk pengisian saldo dompet digital," (AC, 2022)

Selain menggunakan fitur chat pada aplikasi whatssapp, pelaku juga menggunakan fitur panggilan telepon pada aplikasi tersebut. Hal ini sesuai dengan kasus yang pernah terjadi oleh korban MZ dan dr. Binsar. Kedua korban tersebut, dihubungi oleh pelaku penipuan melalui panggilan whatsapp. Kasus korban MZ yang mulanya mendapatkan telfon via whatsapp yang mengatasnamakan BSI yang saat itu pelaku menjelaskan terdapat perarturan baru bahwa biaya transfer akan dikenakan lebih mahal dari biasanya. Selanjutnya korban diperintahkan untuk melengkapi form yang berisi pilihan biaya transfer, kode aktivasi, dan PIN.

Sama hal nya dengan kasus korban yang bernama dr. Binsar, korban ditelfon melalui aplikasi *whatsapp* dengan nomor telepon yang berawalan kode area +1 dengan logo bank plat merah. Selanjutnya pelaku melakukan aksi modusnya yang sudah umum terjadi yaitu mengaku sebagai petugas bank dan mempengaruhi psikologis korban untuk masuk ke dalam jebakannya.

4.3.2 *Social Engineering Attacks*

Serangan *social engineering* dapat terjadi oleh siapa saja, terkhususnya nasabah bank yang merupakan target penipuan dengan sasaran empuk yang cenderung memiliki menyimpan banyak uang di rekening tabungan nya. Tidak heran jika banyak penipuan *social engineering* lebih memburu korban nya sebagai nasabah bank dibandingkan masyarakat umum. Serangan *social engineering* ini menyerang psikologis korban sehingga mudah untuk dilabui oleh pelaku. Dengan demikan pembahasan mengenai *social engineering* sangat luas, namun pada penelitian ini berfokus pada serangan *social engineering* yang terjadi pada nasabah Bank, sehingga perlu diperdalam untuk pembahasan nya. Berikut ini penjelasan yang berkaitan dengan serangan *social engineering* yang disudutkan lagi mengenai jenis serangan social enginnering yang sering terjadi pada nasabah bank, ancaman serangan, serta informasi apa saja yang menjadi incaran para pelaku *social engineering*.

1. Jenis Serangan

Serangan *social engineering* memiliki berbagai teknik penipuan untuk melemahkan korbannya. Namun tidak semua teknik tersebut digunakan untuk menyerang nasabah bank. Umumnya serangan *social engineering* memiliki dua jenis yaitu berbasis interaksi komputer dan berbasis interaksi sosial. Berdasarkan data lapangan, terdapat dua serangan

yang sering terjadi oleh nasabah diantaranya *phising* (serangan berbasis interaksi sosial) dan *skimming* (serangan berbasis interkasi komputer). Berikut penjelasan nya :

a. *Phising*

Serangan *phising* pada umumnya dilakukan oleh pelaku dengan meniru identitas pihak bank yang berpura – berpura memberikan bantuan kepada korban agar mau mengungkapkan informasi pribadi. Serangan *phising* sering ditemukan dalam bentuk tautan link yang dikirim melalui pesan *email, sms* atau *whatsapp* yang berisi formulir identitas nasabah atau situs web palsu yang dimiliki oleh bank tipuan pelaku.

Penyerangan *phising* pernah terjadi di Propinsi Aceh. Saat itu kasus ditangani oleh Polda Aceh yang sudah melakukan penangkapan pada pelaku. Berdasarkan konferensi pers Kabid Humas Polda Aceh Kombes Pol. Winardy, pertama kali pelaku melakukan aksinya dengan melakukan penyamaran sebagai petugas bank, kemudian menawarkan penukaran poin hadiah. Setelah korban percaya dengan pelaku, pelaku mengiming –iming korban, jika korban ingin menukarkan hadiah tersebut korban harus mengisi data nasabah melalui tautan link yang telah dikirim pelaku. Dengan demikian, peneliti menyimpukan bahwa tahap serangan *phising* yang dilakukan oleh pelaku memiliki tiga modus sebelum korban masuk ke dalam link phising yang dikirim oleh pelaku diantaranya :

1) Mengaku sebagai petugas bank
2) Menawarkan hadiah menarik
3) Menarik korban agar percaya dengan pelaku
4) Mengarahkan korban untuk melengkapi data nasabah melalui tautan link

Setelah korban mengisi data nasabah di tautan link tersebut, pelaku berhasil untuk menguasai identitas korban, sehingga pelaku akan mudah untuk mencuri uang di rekening tabungan korban. Hal serupa juga pernah terjadi pada kasus pengambilalihan rekening

JENIUS yang ditangani oleh Polda Metro Jaya. Pengungkapan kasus ini berawal dari laporan dari bank yang mendapat aduan dari nasabah nya bahwa rekeningnya telah terkuras habis oleh pelaku hingga nol. Pelaku berhasil meyakinkan korban untuk mengisi link web *phising* dan menguasai identitas nasabah. Berikut pernyataan Kabid Humas Polda Metro Jaya Kombes Pol Yusri Yunus saat konferensi pers di Polda Metro Jaya :

"Jadi saat OTP keluar otomatis data nasabah diambil alih oleh para pelaku dan kuras habis isi rekening 14 korban. Total kerugian yang dialami nasabah itu ditaksir mencapai Rp 2 Milliar," (Kombes Pol Yusri Yunus, 2021)

Selain itu terdapat kasus yang lain, kasus penangkapan pelaku penipuan seorang warga Palembang yang telah menguras tabungan di rekening korban yang merupakan nasabah bank asal Trenggalek. Bermula pelaku mengaku kepada korban sebagai petugas bank, yang ingin membantu korban agar terselamat dari modus penipuan. Namun pada kenyataan nya, pelaku justru mengarahkan korban untuk masuk ke dalam jebakan nya yaitu korban mengikuti arahan dari pelaku untuk mentransfer uang yang ada di rekening ke dompet digital melalui virtual akun milik pelaku. Berikut keterangan dari pelaku saat konferensi pers dengan Kasat Reskrim Polres Trenggalek Iptu Agus Salim :

"Kemudian saya bilang, sini saya bantu supaya tidak bisa diakses oleh orang lain. Kemudian saya alihkan ke whatsapp dan saya minta untuk mengirimkan kode untuk pengisian saldo dompet digital," (AC, 2022)

Berdasarkan konferensi pers atas kasus – kasus yang pernah terjadi. Peneliti menyimpulkan bahwa terdapat teknik *phising* yang sering dilakukan oleh pelaku untuk memancing korbannya, yaitu :

1) Pesan melalui *email*

Teknik yang sering digunakan oleh pelaku yaitu mengirim email ke semua jutaan nasabah yang mengaku dari Bank resmi. Umumnya email tersebut berisi permintaan nomor kredit, pin OTP, password alun nasabah.

2) Pesan *(Chatting)*

Pesan instan merupakan metode yang digunakan pelaku untuk mengirim pesan yang mengarahkan korban dengan link yang terhubung ke situs web palsu yang tampilan nya hampir sama dengan situs web resmi. Umumnya pelaku menggunakan sms atau aplikasi *whatsapp* untuk mengirimkan pesan instan tersebut.

3) Manipulasi tautan link

Teknik yang digunakan pelaku pada serangan *phising* yaitu pelaku memanipulasi link pada alamat web yang mirip dengan alamat situs web dari bank asli.Website palsu buatan pelaku ketika dibuka seakan – akan seperti website bank asli tetapi bentuknya janggal, tidak mencerminkan website perusahaan. Selain itu, pelaku menggunakan URL yang salah ejaan nya atau penggunaan subdomain untuk mengecoh korban nya, yang hal ini merupakan trik yang sudah umum dilakukan oleh pelaku.

b. *Skimming*

Terdapat beberapa kasus skimming yang pernah terjadi di Kabupaten Bojonegoro. Sudah lima nasabah di Bojonegoro yang melapor bahwa telah terjadinya pencurian data melalui *skimming*. Hal ini ditandai dengan laporan korban yang bernama Aris yang merupakan salah satu nasabah yang kehilangan uang. Aris merasa bahwa tidak pernah melakukan transaksi sama sekali, namun uang di dalam rekening tabungan nya hilang. Sebagaimana hal ini disampaikan oleh Aris selaku korban :

"Kemarin saya mau melakukan transaksi di ATM tetapi saldonya kurang, padahal saldo saya sebelumnya sekitar Rp. 13 juta sekian," (Aris, 2021)

Hal ini terjadi karena nasabah yang kehilangan uang tersebut data nya telah diketahui oleh pelaku *skimming,* yang sebelumnya pelaku telah memasang alat skimming di ATM. Seperti kasus skimming yang terjadi pada tahun 2021 yang pernah dilakukan oleh dua warga Bulgaria yang menjadi pelaku *skimming* di wilayah Jawa Timur. Dua

pelaku tersebut telah memasang alat skimming di ATM yang berada di Jalan Sultan Agung, Pasuruan. Pelaku memasang alat tersebut sejak 26 Juli hingga 31 Juli 2021 dengan total nasabah yang menjadi korban yaitu 29 nasabah. Kemudian data yang telah terlihat oleh pelaku, akan dikirim ke server teman pelaku yang berada di negara asalnya. Setelah itu, data tersebut dikirim kembali dengan analisa nomor kartu dan PIN ATM yang sama, dan dipindahkan ke blank card sehingga sama persis dengan ATM baru. Kapolres Kota Pasuruan AKBP Arman mengatakan bahwa para pelaku telah merencanakan untuk memasang serangkaian perlengkapan alat skimming di setiap mesin ATM yang sering dilewati. Berikut konferensi pers Kapolres Kota Pasuruan :

> "Dua tersangka ini memasang alat skimming di mulut ATM dan *micro cam* (kamera kecil) di atas tombol PIN. Dengan begitu, tersangka bisa mengetahui identitas kartu ATM nasabah dan PIN ATM pada saat dipencet," (AKBP Arman, 2021)

Selain itu, terdapat kasus *skimming* lain yang terjadi pada tahun 2022. Pada kasus ini pelaku *skimming* dilakukan lagi oleh dua pria berwarga Negara Bulgaria dan ditemani oleh dua wanita warga negara Indonesia yang pelakunya berbeda dengan kasus sebelumnya. Pada kasus ini para pelaku melakukan aksinya wilayah kota Manado, pelaku beraksi di 26 lokasi mesin ATM Bank SulutGo di wilayah Kota Manado pada tanggal 30 Juni 2022 sekitar pukul 00:30 hingga 06.00 WITA. Para pelaku sengaja memasang alat itu, untuk mencuri data nasabah berupa PIN pada ATM korban. Kombes Pol Nasriadi yang mendampingi Kapolda Sulut Irjen Pol Mulyatno saat melaksanakan konferensi pres mengatakan bahwa modus *skimming* yang dilakukan pelaku dengan memasang alat di ATM dan dicolok, untuk mendapatkan pin nasabah. Setelah mengetahui PIN korban, pelaku menyalin PIN tersebut untuk mencuri uang di ATM korban dengan memakai kartu buatan pelaku yaitu kartu putih yang berisi *magnetic stripe*. Sebagaimana yang dikatakan oleh Kapolda Sulut Irjen Pol Mulyatno melalui konferensi pres penangkapan dua pelaku *skimming* berwarga negara Bulgaria pada mesin ATM Bank SulutGo, Manado :

"Modus operandinya, para pelaku mengambil uang nasabah dengan cara melakukan transaksi (tarik tunai dan transfer) di mesin – mesin ATM Bank SulutGo dengan menggunakan kartu yang menyerupai kartu ATM (kartu putih yang berisi magnetic stripe)," (Irjen Pol Mulyatno, 2022)

2. Ancaman Serangan

Serangan *social engineering* merupakan jenis serangan yang harus diwaspadai, karena serangan ini dapat terjadi dalam berbagai bentuk yaitu secara online maupun offline. Serangan *social engineering* hadir di tengah masyarakat, karena banyak yang belum menyadari bahwa pentingnya keamanan informasi pribadi yang sifatnya rahasia seperti nomor telepon, PIN OTP, alamat email, password. Lebih lanjut, banyak juga masyarakat yang tidak mengikuti perkembangan teknologi, dan tidak mengetahui ancaman – ancaman yang terjadi di sekitarnya, sehingga masyarakat tidak memiliki pengetahuan untuk memberikan perlindungan terbaik pada informasi pribadi milik nasabah. Dengan demikian perlu bagi nasabah bank untuk mengetahui ancaman – ancaman yang terjadi pada serangan *sosial engineering* ini. Berikut ancaman – ancaman *sosial engineering* berdsarkan data lapangan :

a) Kerugian Keuangan

Dalam kasus penipuan seperti ini, tentunya pelaku penipuan mengincar keuntungan yang didapatkan dari aksi kejahatan nya. Tidak heran jika pelaku memburu korban nya untuk mencuri uang yang dimiliki korban di rekening tabungan nya, sehingga pelaku memiliki berbagai cara agar pelaku berhasil mendapatkan uang milik korban. Berdasarkan data lapangan menunjukan bahwa dampak dari serangan *sosial engineering* ini dapat mengakibatkan kerugian keuangan bagi korban, karena minimnya pengetahuan korban yang kemudian dimanfaatkan oleh pelaku untuk dieksploitasi supaya korban dapat memberikan informasi pribadinya dengan mudah kepada pelaku.

Adapun kasus yang dialami oleh seorang wanita pengusaha asal Cirebon yang menjadi korban tertelannya kartu di mesin ATM, hal ini termasuk aksi kejahatan yang dilakukan oleh pelaku dengan meletakkan alat di mesin ATM untuk menahan kartu korban agar tidak dikeluarkan. Tujuan pelaku melakukan ini agar dapat mengusai kartu korban dan dapat mengaksesnya. Saat itu, korban langsung mengambil buku tabungan nya untuk melakukan proses pemblokiran kepada pihak bank melalui telepon, namun pelaku telah melakukan gerak cepat untuk melakukan pembobolan rekening milik korban, sehingga korban kehilangan uang tabungan nya sebesar Rp. 70 juta. Sebagaimana yang diungkapkan oleh korban sebagai berikut :

"Uang saya sudah hilang Rp. 70 juta. Saya kaget, mangkanya saya langsung ke Bank BNI Cangkol. Ternyata benar, hilang uang saya," (Iin Kristina, 2021)

Serupa dengan kasus diatas, masih terdapat kasus lain yang mengalami kerugian atas penipuan *social engineering* ini. Kasus penipuan ini menimpa seorang ketua KPU Sidoarjo Muhammad Iskak yang menjadi korban modus ganjal ATM. Saat korban ke ATM untuk mengambil uang, korban selalu gagal untuk memasukkan kartu nya, dan pada akhirnya kartu nya pun tersangkut. Pada saat kejadian, bersamaan juga munculnya seorang yang tidak dikenal yang menawarkan bantuan kepada korban, merasa ada yang tidak beres, korban langsung menuju kantor cabang bank terdekat. Namun, saat dalam perjalanan menuju bank korban mendapatkan notifikasi melalui SMS banking bahwa telah dilakukan transkasi keluar pada rekening tabungan nya. Dalam kasus ini korban telah kehilangan uangnya sebesar Rp 36.800.000. Sebagaimana yang disampaikan oleh korban :

"Sudah saya laporkan. Mereka memang sepertinya sudah mengintai saya sejak saya masuk ATM. Kerugiannya ada tujuh kali tarik tunai Rp 1.250.000 lalu sekali tarik Rp 1 juta dan transfer ke luar rekening dua kali sebesar Rp 10 juta dan Rp 17 Juta sehingga total Rp 36,8 juta," (Muhammad Iskak, 2021)

Selain itu pada kasus yang lain, korban penipuan *social engineering* ada yang mengalami kerugian hingga ratusan juta. Seperti kasus yang terjadi pada warga Sleman yang menjadi korban penipuan dengan modus pelaku yang menyamar sebagai petugas bank. Berawal pelaku menelfon korban dan melakukan bujuk rayu untuk memberikan data pribadinya. Akibat penipuan ini tabungan korban hilang sebesar Rp. 510.000.000 yang berpindah ke rekening pelaku. Penipuan ini termasuk salah satu serangan social engineering sebagaimana yang dikatakan oleh AKBP Roberto Gomgom Manorang Pasaribu :

> "Metodenya kita kenal dengan nama *social engineering*, pelaku mencoba melakukan bujuk rayu kemudian menelpon korban," (AKBP Roberto Gomgom Manorang Pasaribu, 2021)

Selanjutnya, terdapat kasus yang berbeda dari sebelumnya. Kasus kali ini pelaku menggunakan modus menawarkan iklan upgrade menjadi nasabah prioritas di bank dengan rayuan promosi. Korban yang terperangkap pada jebakan pelaku diminta memberikan data pribadi seperti nomor ATM, PIN, OTP, Nomor CVV/CVC dan password. Pelaku yang beroperasi di Sumatera Selatan telah ditangkap oleh Polda Metro Jaya. Pada konferensi pers disebutkan bahwa dalam kasus ini pelaku berhasil menggasak uang korban sebesar Rp. 181.000.000 . Sebagaimana yang disampaikan oleh Kanit 2 Resmob Ditreskrimum Polda Metro Jaya Komisaris Maulana Mukarom :

> "Dalam perkara ini kerugian korban yang dinikmati pelaku Rp 181 juta. Tapi kita tidak berhenti di sini, kita masih mendalami, cari pelaku – pelaku lain dan dari Subdit Resmob terus mengembangkan pengungkapan sindikat ini," (Komisaris Maulana Mukarom, 2022)

Berdasarkan kasus – kasus diatas, pelaku mengincar uang korban tidak sedikit, selama terbuka kesempatan untuk menipu, pelaku memanfaatkan peluang tersebut. Berbeda dengan kasus sebelumnya, kerugian yang dialami korban hingga ratusan juta rupiah, namun dalam kasus ini pelaku berhasil meraub keuntungan hingga milliaran

rupiah. Kasus ini terjadi di Kota Manado, kasus ini melibatkan beberapa pelaku diantara nya dua pria warga negara Bulgaria dan dua wanita warga negara Indonesia. Para pelaku tersebut melakukan aksi kejahatan skimming di beberapa ATM Bank SulutGo dengan memasang alat skimmer dalam card reader di mesin ATM. Aksi kejahatan pelaku ini berhasil mengumpukan uang sejumlah Rp 1.789.563.000 dari 144 rekening nasabah Bank SulutGo. Hal ini sesuai konferensi pers yang disampaikan oleh Irjen Pol Mulyatno :

> "Sebelumnya pada bulan Januari 2022, ditemukan alat skimmer dalam card reader mesin ATM Bank SulutGo Markobar Tikala, Manado, dan pada bulan Maret 2022 para pelaku melakukan transaksi (tarik tunai dan transfer) di beberapa mesin ATM bank lain di wilayah Bali dan Surabaya sejumlah Rp 1.789.563.000 dari 144 rekening nasabah Bank SulutGo yang menjadi korban," (Irjen Pol Mulyatno, 2022)

b) Pencurian Identitas

Salah satu kejahatan yang umum dilakukan oleh pelaku *social engineering* adalah mencuri identitas nasabah. Pencurian identitas merupakan sebuah kejahatan yang sengaja menggunakan identitas orang lain yang bertujuan mendapatkan keuntungan secara finansial dan berbagai manfaat lainnya dengan mengatasnamakan orang lain yang memiliki identitas tersebut. Adapun pencurian identitas yang digunakan pelaku seperti informasi personal orang lain diantaranya nama, nomor kartu kredit, PIN, OTP, password, email. Pelaku mendapatkan itu semua tanpa meminta persetujuan dari sang pemiliki, karena pelaku berniat untuk mencuri dan dimanfaatkan untuk kejahatan penipuan atau kejahatan lainnya.

Pencurian data ini dapat ditemukan pada kejahatan *skimming* di ATM. Berdasarkan kasus – kasus sebelumnya pada kejahatan *skimming*, pelaku telah memasang alat *micro cam* di atas tombol PIN ATM sehingga pelaku dapat melihat PIN nasabah ketika dimasukkan. Seperti kasus penangkapan dua warga negara Bulgaria yang menjadi pelaku *skimming* di Pasuruan. Para pelaku memasang alat skimming di mulut ATM dan

micro cam di ATM, dan setelah para pelaku mengetahui data nasabah, pelaku mengirim data tersebut ke server teman pelaku yang berada di negara asalnya. Sebagaimana konferensi pers yang disampaikan oleh AKBP Arman selaku Kapolres Kota Pasuruan :

"Dua tersangka ini memasang alat skimming di mulut ATM dan *micro cam* (kamera kecil) di atas tombol PIN. Dengan begitu, tersangka bisa mengetahui identitas kartu ATM nasabah dan PIN ATM pada saat dipencet," (AKBP Arman, 2021)

Selain itu terdapat kasus lainnya masih dengan pencurian identitas yaitu kasus pengambilalihan akun milik nasabah bank. Modus yang dilakukan oleh pelaku saat itu adalah mengaku sebagai petugas bank dan mengarahkan korban untuk mengisi data melalui web. Pada akhirnya pelaku berhasil meyakinkan korban untuk mengisi link web yang berisi identitas nasabah. Setelah data nasabah diketahui olek pelaku, pelaku langsung mengambil alih semua alih dan menguras isi rekening milik korban. sebagaimana yang dikatakan oleh Kombes Pol Yusri Yunus saat konferensi pers di Polda Metro Jaya :

"Jadi saat OTP keluar otomatis data nasabah diambil alih oleh para pelaku dan kuras habis isi rekening 14 korban. Total kerugian yang dialami nasabah itu ditaksir mencapai Rp 2 Milliar,"

3. Informasi Incaran Pelaku

a. Data Pribadi Nasabah

Data pribadi nasabah memiliki sifat rahasia dan penting, sehingga diperlukan perlindungan atas keamanan nya. Jika data nasabah tidak diberikan perlindungan keamanan nya, maka orang lain akan mudah untuk mengakses dan mempelajari kondisi keuangan nasabah, yang nantinya dapat disalahgunakan oleh orang lain seperti pencurian uang di rekening nasabah.

Seperti kasus yang diselidiki oleh Polda Metro Jaya, yang berhasil menangkap pelaku penipuan nasabah bank dengan menggunakan modus yang sudah umum yaitu

berpura – pura menjadi petugas bank. Saat itu pelaku yang menghubungi korban, kemudian pelaku melakukan bujuk rayu dan mempengaruhi korban untuk mengikuti perintah nya agar dapat mengisi data nasabah. Korban yang saat itu sudah terpengaruh oleh pelaku, korban akhirnya mengisi data tersebut dan mengirimkan kembali ke pelaku. Sebagaimana yang disampaikan oleh Humas Polda Metro Jaya Kombes Pol Yusri Yunus :

> "Korban yang terpengaruh kemudian mengikuti petunjuk terduga pelaku dengan mengirimkan login terdaftar dengan mengisi data nasabah dan OTP. Setelah pelaku mendapat akun nasabah, pelaku mengambil alih rekening nasabah kemudian dikuras habus," (Kombes Pol Yusri Yunus, 2021)

Berdasarkan kasus diatas, pelaku mengincar data nasabah agar dapat menguasai isi rekening tabungan korban. Banyak korban yang tidak sadar bahwa data nasabah merupakan hal yang sangat rahasia karena nya tidak semua orang boleh untuk mengetahui data tersebut. Bahkan karena sifat nya terlalu penting dan rahasia, ada oknum yang memperjual belikan data nasabah. Seperti kasus penangkapan delapan tersangka pembobol rekening milik Ilham Bintang oleh Polda Metro Jaya. Para tersangka ini memiliki peran yang berbeda – beda ketika melaksanakan aksi kejahatan nya, diantaranya ada yang memiliki tugas memperjual belikan data nasabah, menduplikat SIM card korban hingga menguras habis uang di rekening korban. Bermula polisi menangkap pelaku D yang menjadi otak kejahatan ini, Kabid Humas Polda Metro Jaya Kombes Yusri Yunus mengatakan bahwa pelaku D merupakan bos dari sindikat kasus ini. Pelaku D membeli data – data nasabah bank dan slip OJK untuk mengetahui data – data korban sebagai targetnya. Pelaku D membeli data – data nasabah dari pelaku H yang merupakan pegawai bank yang bekerja di salah satu bank di Jakarta. Sebagaimana yang dikatakan oleh Kombes Pol Yusri Yunus :

"H laki – laki, dia bekerja di salah satu bank di Jakarta ini BPR. Tersangka H punya akses bisa dapat SLIK OJK atau slip OJK. Disitu ada data – data pribadi lengkap seseorang yang memiliki rekening atau limit rekening," (Kombes Pol Yusri Yunus, 2020)

"Dia menggunakan kewenangannya ini untuk berbuat jahat, dia menjual ke orang – orang yang enggak bertanggung jawab termasuk ke D," (Kombes Pol Yusri Yunus, 2020)

b. OTP

Kode OTP singkatan dari *one time password* yang merupakan suatu lapisan keamanan saat bertransaksi online perbankan. Kode OTP ini sifatnya sangat rahasia dan tidak boleh diberikan kepada siapa pun. Fungsi kode OTP yaitu memperkuat lapisan keamanan transaksi keuangan online setelah PIN dan password.

Dengan demikian, kode OTP ini sangat diincar oleh pelaku karena dengan mengetahui kode OTP nasabah, pelaku dapat menguasai akun nasabah , sehingga pelaku dapat menguras uang tabungan di rekening nasabah. Seperti kasus yang dialami oleh warga Sleman yang ditelpon oleh seseorang yang mengaku sebagai petugas bank dan bermodus untuk membantu korban menutup aplikasi berbayar. Pelaku melakukan bujuk rayu kepada korban, dan mengarahkan korban untuk mengirimkan kode aktivasi aplikasi atau kode OTP. Tidak lama kemudian muncul SMS ada permintaan *one time password* (OTP) atau kode akses untuk password yang dimiliki oleh aplikasi yang nanti akan diakses oleh pelaku atau tidak berdasarkan otorisasi. Setelah dibujuk rayu oleh pelaku selama tiga kali agar dapat memberikan kode OTP, korban pun memberikan kode OTP tersebut kepada pelaku. Setelah beberapa jam kemudian, korban mendapatkan notifikasi melalui SMS bahwa telah terjadi transaksi keluar yang dilakukan oleh pelaku.

Selanjutnya, terdapat kasus lainnya yang serupa dengan kasus diatas yaitu kasus penipuan online kepada nasabah bank di Provinsi Aceh. Kasus ini bermula, pelaku melakukan modus menghubungi korban yang mengaku sebagi petugas bank dan kemudian menawarkan penukaran poin hadiah. Kemudian pelaku melakukan bujuk rayu

nasabah disertai dengan pengiriman link untuk permintaan data nasabah dan kode OTP atau kode aktivasi *mobile banking*. Sebagaimana yang diungkapkan oleh Kabid Humas Polda Aceh Kombes Pol Winardy melalui konferensi persnya :

"Modusnya adalah pengiriman link untuk permintaan data nasabah. Setelah itu, pelaku melakukan permintaan OTP atau kode aktivasi *mobile banking*," (Kombes Pol Winardy, 2022)

4.4 Pola – Pola Strategi Sosialisasi Pencegahan Penipuan *Social Engineering* Oleh Bank Melalui Media Website dan Media Sosial Twitter

Dewasa ini teknologi yang semakin berkembang telah mencapai titik puncaknya. Munculnya teknologi digital yang memiliki fitur – fitur di dalam nya mengukur perkembangan teknologi semakin berkembang, terutama teknologi yang berbasis internet yang membuat jarak dan waktu lebih dapat dihemat karena hadirnya perkembangan teknologi informasi yang kini hadir. Aktivitas yang memerlukan waktu lama dan jarak yang jauh dapat dikerjakan atau diakses dimana pun hanya hitungan detik. Sebagaimana dengan teknologi yang berbasis internet, dengan adanya sistem yang telah tekomputerasasi pengoperiasan nya serba otomatis dan canggih.

Oleh karena itu, perkembangan teknologi ini dapat dimanfaatkan sebagai sarana untuk melakukan langkah – langkah pencegahan penipuan *social engineering* pada nasabah perbankan. Apalagi dengan hadirnya perkembangan teknologi yang membuat semua aktivitas menjadi mudah untuk diterapkan. Pencegahan penipuan *social engineering* perlu untuk ditindaklanjuti, agar kasus penipuan *social engineering* tidak semakin meningkat. Jika dikaitkan dengan teori *crime triangle*, keberadaan elemen *controller* yang diposisikan oleh bank memiliki peran penting untuk mengatasi suatu masalah yang dialami oleh nasabah bank yang menjadi korban penipuan.

Dengan demikian perlu adanya langkah – langkah pencegahan untuk mengatasi hal tersebut. Saat ini banyak cara yang dilakukan oleh bank – bank di Indonesia sebagai

tindakan pencegahan untuk mengatasi kasus penipuan *social engineering,* seperti penggunaan fitur – fitur kemanan di kartu debit dan bank juga dapat memberikan sosialisasi mengenai penipuan *social engineering* yang umumnya dibagikan melalui media *offline* ataupun *online.* Sosialisasi lewat media *offline* yang artinya bahwa sosialisasi dilakukan bertatap muka dengan nasabah, sedangkan sosialisasi melalui media *online* mengartikan bahwa sosialisasi yang diberikan hanya bisa diakses menggunakan jaringan internet sebagai sarana untuk berkomunikasi secara *online* melalui media *website* dan media sosial *twitter*. Penggunaan media online sebagai media sosialisasi merupakan hal yang tepat untuk diterapkan, karena proses menjadi lebih mudah, efektif dan efisien. Selain itu, jika dikaitkan dengan teori *gullibility*, pemberian sosialisasi ini dapat mengurangi unsur *gullibility* pada nasabah, karena dapat memperkuat cara berfikir (*cognition*) nasabah dengan bertambahnya pengetahuan mengenai modus *social engineering* dan nasabah tidak mudah terjebak dalam unsur *situation* yang telah di rancangan oleh pelaku.

Oleh karena itu peneliti tertarik untuk menganalisa pencegahan penipuan *social engineering.* Namun, dalam penelitian ini memiliki batasan penelitian supaya dalam penelitian ini lebih mendekatkan pada pokok permasalahan yang akan dibahas. Hal ini agar tidak terjadi pembahasan masalah yang terlalu luas atau lebar yang dapat mengakibatkan penelitian itu tidak dapat fokus atau kerancuan dalam menginterpretasikan hasil penelitian.

Dengan demikian dalam penelitian ini, peneliti memilih untuk menganalisa pola – pola strategi sosialisasi pencegahan penipuan *social engineering* melalui media website dan media sosial twitter yang diberikan oleh bank – bank besar di Indonesia. Adapun bank – bank tersebut diantara nya Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Permata, Bank Rakyat Indonesia (BRI), Bank Syariah Indonesia (BSI). Alasan peneliti memilih bank – bank tersebut yaitu berdasarkan bank – bank yang

memiliki *asset* besar di Indonesia dan bank – bank yang sering digunakan oleh pelaku penipuan sebagai penyamaran identitasnya. Selanjutnya peneliti akan memaparkan pola – pola strategi sosialisasi pencegahan penipuan *social engineering,*yang telah peneliti ambil dari website dan media sosial twitter menggunakan *NCapture* fitur bawaan dari Software NVivo, yang telah peneliti jelaskan dalam uraian – uraian berikut ini :

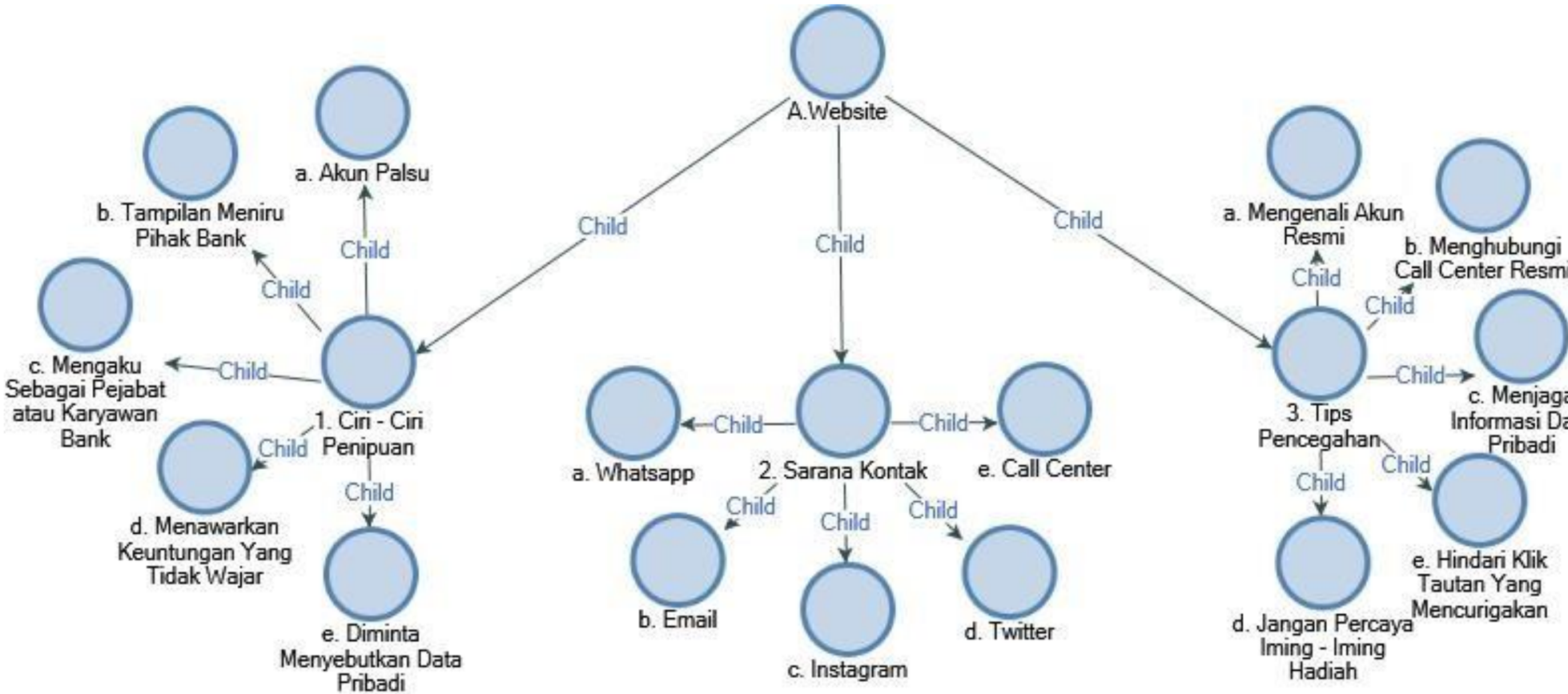
4.4.1 Website

Hadirnya penipuan *social engineering* membuat bank – bank di Indonesia memberikan sebuah langkah pencegahan penipuan. Maraknya penipuan *social engineering* yang sebagian telah terjadi di Indonesia, mengharuskan bank untuk memberikan langkah pencegahan penipuan kepada seluruh masyarakat Indonesia dengan cara yang efektif dan efisien.

Bank – bank di Indonesia hampir semuanya menggunakan situs website perusahaan sebagai media untuk menyalurkan sosialisasi pencegahan penipuan *sosial engineering*. Penggunaan situs website sebagai media sosialisasi merupakan hal yang tepat untuk diterapkan karena hidup di zaman perkembangan teknologi ini membuat semua kegiatan lebih mudah, efektif dan efisien.

Pada bagian ini, peneliti akan menjelaskan pola - pola sosialisasi pencegahan penipuan *social engineering* yang telah peneliti rangkum dari berbagai situs website bank resmi diantaranya Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Permata, Bank Rakyat Indonesia (BRI), Bank Syariah Indonesia (BSI). Sosialisasi pencegahan penipuan *sosial engineering* melalui media website bank resmi dapat dilihat dari hasil analisa yang telah peneliti olah menggunakan software NVivo 12 yang terdapat pada Gambar IV.9 :

Gambar IV. 8 Peta Analisa Pola – Pola Strategi Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Website



Sumber : Diolah Peneliti Menggunakan NVivo 12

Tabel IV. 2 *Matrix Coding* Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Website* (Berdasarkan Jumlah Kata)

Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Website*	BCA	BNI	BRI	BSI	MANDIRI	PERMATA
1. Ciri - Ciri Penipuan	0	0	0	0	0	0
a. Akun Palsu	205	0	82	0	0	0
b. Tampilan Meniru Pihak Bank	143	14	0	0	0	0
c. Mengaku Sebagai Pejabat atau Karyawan Bank	143	0	244	45	35	90
d. Menawarkan Keuntungan Yang Tidak Wajar	52	0	0	0	35	33
e. Diminta Menyebutkan Data Pribadi	171	22	100	94	0	0
2. Sarana Kontak	138	37	0	13	5	0
a. Whatsapp	8	0	305	0	0	0
b. Email	7	0	171	16	15	3
c. Instagram	22	0	69	52	0	1
d. Twitter	8	0	0	52	11	1
e. Call Center	84	61	69	16	5	3
3. Langkah – Langkah Pencegahan	879	494	0	152	372	204
a. Mengenali Akun Resmi	505	67	66	45	25	0
b. Menghubungi Call Center Resmi	120	55	209	0	31	0
c. Menjaga Informasi Data Pribadi	185	44	137	49	85	78
d. Jangan Percaya Iming - Iming Hadiah	21	58	0	45	0	0
e. Hindari Klik Tautan Yang Mencurigakan	0	17	0	0	31	0

Sumber : Diolah Peneliti Menggunakan NVivo 12

Gambar IV.9 dan Tabel IV.2 merupakan informasi *coding* yang dihasilkan saat mengolah hasil data *NCapture* website bank resmi yang telah peneliti olah menggunakan bantuan *Software NVivo 12*. Gambar dan tabel tersebut memaparkan pola – pola strategi sosialisasi pencegahan penipuan *social engineering* menggunakan website. Adapun hasil *coding* pada tabel IV.2 memberikan keterangan "angka" yang artinya banyaknya jumlah kata – kata yang sering muncul dari poin – poin sosialisasi pencegahan penipuan *social engineering* melalui website. Lebih lanjut peneliti akan menginterpretasi hasil analisis tersebut ke dalam uraian – uraian berikut ini :

1. Bank Central Asia (BCA)

Sudah menjadi perhatian umum, ketika pelaku ingin melakukan kejahatan penipuan, pelaku membuat akun palsu terlebih dahulu agar orang – orang tidak mengenali identitas nya. Berdasarkan informasi yang diambil dari website Bank BCA, terdapat beberapa indikator untuk mengenali akun palsu diantara nya :

1) Akun palsu yang mengatasnamakan dan menggunakan logo yang sama dengan bank resmi.
2) *Email e-statement* dan notifkasi tidak resmi. Pelaku akan mengirimkan email yang mirip dengan e-mail bank terkait *billing statement.*
3) Pelaku akan mendekati korban nya melalui sosial media atau aplikasi *whatsapp* yang di desain mirip dengen akun bank asli.
4) Pelaku sering mengaku sebagai *call center* bank resmi, bahkan pelaku juga memasang iklan di halaman pencarian google dengan nama akun palsu yang

5) dibuat pelaku disertai dengan nomer *whatsapp* pelaku sebagai *call center* palsu.

6) Pelaku akan mencantumkan tautan link di bio Instagram akun palsu nya, yang tautan link tersebut akan terhubung langsung di kontak *whatsapp* pelaku.

7) Alamat *email* milik pelaku biasanya mirip atau serupa tapi tidak sama dengan email resmi.

8) Nomor telepon palsu umumnya diawali dengan kode area seperti 021-1500888, +621500888, dan lain nya

9) Akun *whatsapp* milik pelaku penipuan umumnya tanpa ada centang hijau yang menandakan akun tidak terverifikasi.

Berdasarkan informasi melalui laman website resmi bank BCA (www.bca.co.id) website palsu buatan pelaku bentuknya janggal, memang pelaku mendesain website tersebut mirip dengan yang asli. Namun bentuknya website nya berantakan. Selain itu, pelaku juga akan mencantumkan *call center* palsu di halaman website nya, dimana *call center* tersebut langsung terhubung ke *whatsapp* pelaku.

Dalam melancarkan aksinya, pelaku tentunya memiliki berbagai macam modus untuk menglabui korban nya. Umumnya pelaku berpura- pura menjadi petugas bank agar korban percaya dengan pelaku, sehingga tertarik dengan tawaran, arahan yang diberikan oleh pelaku. Dalam rangka untuk mengenali modus tersebut, Bank Central Asia (BCA) memberikan sosialisasinya terkait modus ini yang dibagikan melalui website resmi nya, diantaranya :

1) Biasanya pelaku penipuan mengkalim legalitas mengatasnamakan OJK/ mencatut nama pejabat BCA sebagai admin group dalam aplikasi chat,

2) Pelaku aktif mengontak korban via telepon, chat, medsos, atau media lainnya. Kemudian mengiming – iming korban, mengaku dari bank atau pihak tertentu sehingga korban mudah percaya,

3) Pelaku yang berhasil mengakses myBCA milik korban dan mengetahui semua informasi di dalamnya, pelaku penipuan akan menghubungi korban melalui bermacam - macam sarana seperti telepon, chat, dan mengaku dari bank BCA,

4) Terdapat modus penipuan yang lain yang mengatasnamakan BCA dan berpura – pura menawarkan korban bantuan untuk membuat BCA ID, menghubungkan ke semua rekening BCA, serta memberikan link pembebasan admin fee. Padahal ini adalah upaya mendapatkan data – data pribadi dengan tujuan mengakses transaksi finansial nasabah.

Adapun pelaku penipuan yang menawarkan keuntungan yang tidak wajar, untuk menarik perhatian korban nya. Berikut ini akan dipaparkan informasi yang diberikan oleh Bank Central Asia (BCA) modus yang sering dilakukan oleh pelaku saat menawarkan keuntungan yang tidak wajar :

1) Pelaku menjajikan bagi hasil investasi yang tidak wajar atau tidak masuk akal,

2) Pelaku menginformasikan terdapat transaksi penggunaan kartu kredit yang tidak wajar,

3) Pelaku menebar website atau *online shop* bodong dan menawarkan investasi atau arisan online dengan iming – iming profit yang menggiurkan korban,

Pada akhirnya dari segala modus yang dilakukan, tujuan utama pelaku penipuan adalah mendapatkan data nasabah. Adapun modus yang sering digunakan oleh pelaku untuk meminta data nasabah yang dimuat melalui website resmi BCA, yaitu :

1) Pelaku mencoba untuk mendapatkan data nasabah seperti nomer kartu kredit, exp date, dan CVV, pelaku melalui link atau attachment yang dikirimkan melalui email,

2) Pelaku mengarahkan korban untuk input data – data pribadi ke web palsu melalui *chat whatsapp* dengan akun BCA palsu milik pelaku,

3) Email resmi tidak pernah memberikan link apapun. Email palsu biasanya memberikan link agar korban mengisi data pribadi,

4) Pelaku akan bersilat lidah dengan melakukan teknik *social engineering* agar korban mau memberikan data pribadi,

Dengan demikian, jika nasabah menemukan akun palsu atau tanda – tanda penipuan, maka nasabah dapat lapor atau konfirmasi terlebih dahulu ke sarana kontak bank. Berikut ini Bank Central Asia (BCA) telah memberikan layanan sarana kontak yang dapat dihubingi oleh nasabah, diantaranya :

1) *Call Center* : Halo BCA 1500 888 , tidak ada awalan 021, +62, atau lainnya

2) *Email* : halobca@bca.co.id

3) *Instagram* : @goodlifebca

4) *Twitter* : @BankBCA

5) *Whatsapp* : 62-811-1500-998

Selain itu, Bank Central Asia (BCA) juga memberikan langkah – langkah pencegahan di halaman websitenya. Hal ini ditunjukkan pada tabel IV.2 yang membuktikan bahwa Bank Central Asia (BCA) banyak memberikan langkah – langkah pencegahan penipuan yang ditandai dengan banyaknya jumlah kata yang sering muncul dalam halaman web nya yaitu 879 kata. Jumlah kata "langkah – langkah pencegahan penipuan" dihalaman website BCA memiliki jumlah kata terbanyak dibandingkan dari bank – bank lainnya.

2. Bank Negara Indonesia (BNI)

Umumnya pelaku penipuan menyamarkan identitasnya dengan mengaku sebagai petugas bank. Sosialisasi yang diberikan oleh Bank Negara Indonesia membahas terkait

dengan penyamaran identitas pelaku penipuan dengan membuat situs web palsu yang memiliki alamat dan tampilan mirip dengan situs resmi milik bank. Hal ini dilakukan oleh pelaku untuk mengecoh korban nya agar korban percaya dengan pelaku.

Setelah itu,BNI juga memberikan sosialisasi mengenai ciri – ciri penipuan yang meminta data nasabah. Berdasarkan informasi yang di dapat dari website, BNI memberikan himbauan untuk waspada terhadap serangan phising, pelaku yang mengarahkan korban untuk menyebutkan data pribadi. Supaya dapat mengenali modus tersebut,BNI memberikan cara agar dapat mengenalinya yaitu mengenali email atau sms yang menginfomasikan URL link atau login screen atau meminta login dengan cara memasukkan user ID dan PIN.

Dalam halaman website nya, BNI menghimbau kepada nasabah nya agar menjaga informasi data kartu kredit seperti nomor kartu kredit, masa berlaku, nomo CVV/CVC, OTP (*One Time Password*), dan identitas pribadi lainnya kepada siapapun, termasuk kepada pegawai BNI. Selain itu, dalam sosialisasinya BNI mengajak nasabah nya untuk melaporkan jika mengalami hal – hal yang mencurigakan dan segera laporkan ke nomor resmi BNI *Call* 1500046.

3. Bank Rakyat Indonesia (BRI)

Sosialisasi yang diberikan oleh Bank Rakyat Indonesia (BRI) mengenai pencegahan penipuan *social engineering* yaitu memberikan himbauan kepada nasabah nya agar tetap menjaga informasi pribadi, jangan pernah memberikan informasi kepada siapa pun termasuk orang yang mengaku sebagai pihak bank. BRI mengingatkan bahwa akun resmi *whatsapp* BRI tidak pernah meminta data nasabah dalam berkomunikasi. Kemudian, BRI memberikan sosialisasi untuk mengenali akun palsu whatsapp yang mengatasnamakan BRI diantara nya :

1) Menggunakan nomor ponsel palsu(WA resmi BRI Sabrina hanya 0812-12-14017

2) Tidak memiliki logo verified atau centang hijau

3) Profile picture menyerupai akun resmi namun dalam kualitas rendah

4) Berpura – pura menawarkan bantuan terkait masalah perbankan

5) Menyarankan nasabah untuk mengakses link website BRImo palsu

6) Menyarankan nasabah untuk memberitahukan data pribadi seperti OTP, CVV/CVC, PIN atau password

Dalam sosialisasinya, BRI juga mensosialisasikan layana saran kontak bagi nasabah, jika terjadi kejanggalan atau terdapat hal yang tidak wajar . Berikut akun resmi BRI yang harus diketahui oleh nasabah :

1) Call Center : 14017/1500017

2) Whatsapp (Sabrina) / SMS : 0812-12-14017

3) Twitter : @BANKBRI_ID, @kontakBRI, @promo_BRI Instagram

4) Tiktok : bankbri_id

5) Youtube : BANK BRI

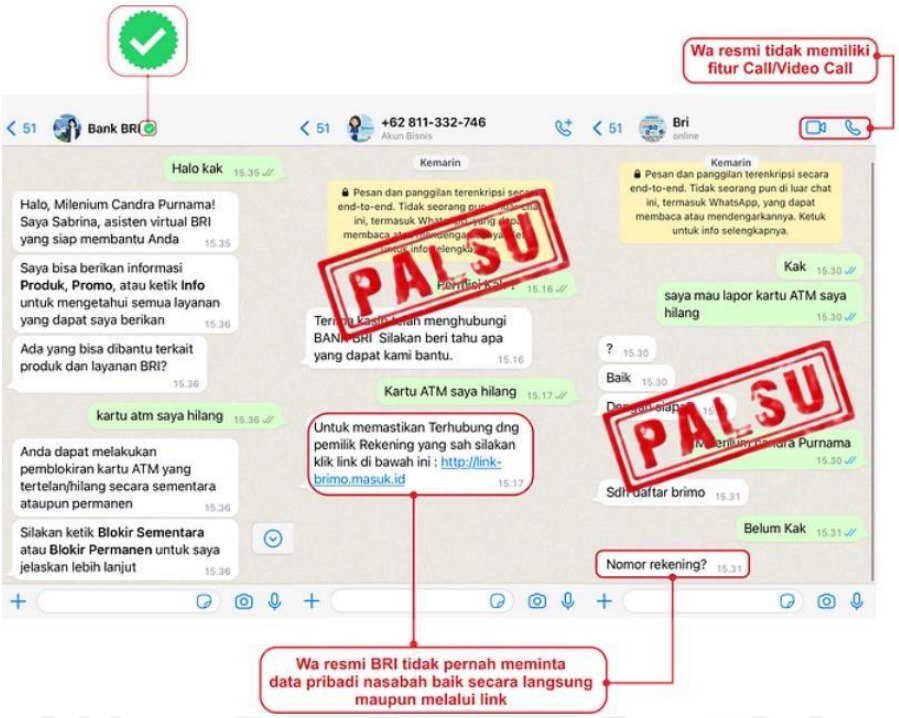
6) Facebook Messenger (Sabrina) : BANK BRI

7) Email BRI : callbri@bri.co.id

8) Instagram : @bankbri_id

Sebagai upaya pencegahan penipuan s*ocial engineering,* BRI juga mensosialisasikan mengenai penting nya untuk mengenali ciri – ciri akun palsu. Sosialisasi yang diberikan ini dibagikan lewat poster yang terdapat dalam halaman web nya. Berikut ini salah satu poster sosialisasi BRI mengenai akun palsu whatsapp yang terdapat dalam gambar IV.10 :

Gambar IV. 9 Akun Whatsapp Bank Palsu



Sumber : bri.co.id

Dengan demikian, perlu untuk dapat mengenali bahwa akun *whatsapp* BRI yang resmi terdapat ceklist hijau di samping nama kontak yang menandakan bahwa akun whatsapp ini terlah terverifikasi secara resmi. Centang hijau pada akun whatsapp mengkonfirmasi bahwa akun ini merupakan akun bisnis yang dikenal dan autentik.

4. Bank Syariah Indonesia (BSI)

Upaya untuk mencegah penipuan *social engineering*, BSI melakukan preventif dengan memberikan sosialisasi yang berkaitan dengan penipuan. Sosialisasi yang diberikan BSI dapat berupa himbauan kepada nasabah nya agar lebih waspada terhadap segala bentuk penawaran , program promo maupun ajakan untuk mengisi data atau meminta email dan kata sandi yang mengatasnamakan pihak Bank Sinarmas, jika bukan dari situs resmi BSI yaitu www.bankbsi.co.id. BSI juga mensosialisasikan melalui

halaman website nya untuk menjaga kerahasiaan data pribadi, dan jangan pernah memberikan informasi penting kepada siapapun seperti nomor kartu identitas, *username email* beserta kartu sandi, nomor kartu kredit/debit , PIN, ATM, OTP, serta PIN yang sering dipakai di BSI *Mobile.*

Selain itu, BSI juga mensosialisasikan mengenai ciri – ciri akun palsu. Adapun ciri – cirinya, sebagai berikut :

1) Akun media sosial palsu yang mengatasnamakan BSI umumnya tidka ada logo verified atau centang bru di samping username,
2) Profile picture tidak jelas atau buram,
3) Jumlah followers dan postingan sedikit

Jika menurut nasabah ada yang mencurigakan, diharapkan untuk konfirmasi terlebih dahulu kepada BSI. BSI juga mensosialisasikan layanan kontak yang dapat dihubungi nasabah jika diperlukan bantuan, diantaranya :

1) BSI *Customer Care :* 14040
2) Email : contactus@bankbsi.co.id
3) Instagram : @banksyariahindonesia, @lifewhitbsi, & @bsimobile
4) Facebook : banksyariahindonesia
5) Twitter : @bankbsi_id & @bsihelp

5. Bank Mandiri

Pencegahan penipuan *social engineering* pada nasabah dapat dilakukan dengan berbagai upaya. Bank Mandiri yang menjadi bank pilihan nasabah nya melakukan berbagai upaya untuk mencegah penipua tersebut. Salah satunya Bank Mandiri memberikan sosialisasi terkait dengan pencegahan penipuan *social engineering* melalui situs website nya. Bank Mandiri mensosialisasikan bahwa pelaku penipuan dapat

menghubungi nasabah dan mengaku sebagai representatif bank atau orang yang dikenal, dengan modus pembaruan data perbankan nasabah ataupun penawaran suatu hadiah, sehingga nasabah percaya untuk membuka informasi rahasia tersebut.

Lebih lanjut, Bank Mandiri memberikan prinsip Hati – Hati, Teliti, dan Konfirmasi. Adapun indikator – indikator di dalam nya sebagai berikut :

a. Hati – Hati

1) Jangan berikan data kartu kredit dan kartu debit seperti PIN, masa berlaku kartu, 3 angka CVV dibelakang kartu, limit kartu, User ID, kata sandi, dan OTP kepada pihak-pihak yang tidak berkepentingan.
2) Gunakan PIN untuk mengotorisasi transaksi kartu kredit dan kartu Debit di EDC.
3) Ganti PIN dan password secara rutin, terutama apabila belum pernah mengganti password. Gunakan kombinasi huruf kapital, huruf kecil simbol, dan angka. Jangan gunakan password default, tanggal lahir, Nomor HP, atau informasi pribadi lainnya.
4) Terima OTP tapi tidak transaksi, mungkin akun nasabah digunakan orang lain tanpa izin. Segera hapus kartu debit dan kartu kredit dari akun *ecommerce.*
5) Hindari klik tautan yang mencurigakan dari website, email, atau pesan dari orang yang tidak dikenal. Selalu periksa identitas pengirim pesan untuk memastikan pesan tersebut sah dari akun resmi *ecommerce*
6) Simpan kartu kredit atau kartu debit serta data informasi yang ada di dalamnya di tempat yang aman.
7) Hindari login di perangkat yang bukan milik nasabah. Gunakan komputer atau perangkat mobile pribadi saat bertransaksi online untuk mengurangi risiko pencurian *password* dan informasi pribadi lain.

b. Teliti

1) Segera tandatangani bagian belakang kartu yang baru nasabah terima,
2) Pantau histori transaksi kartu debit dan kartu kredit Anda di Livin' by Mandiri secara rutin. Untuk informasi transaksi lebih aktual, aktifkan notifikasi mutasi rekening melalui SMS atau Whatsapp (WA),
3) Pastikan alamat situs yang nasabah akses adalah resmi milik bank ataupun situs belanja online yang tepat untuk menghindari pencurian data kartu kredit dan kartu debit Anda. Tips: lakukan perbandingan dengan hasil Google / Bing / Yahoo search untuk lebih memastikan alamat yang nasabah akses adalah alamat yang resmi,
4) Sebelum menyetujui transaksi, pastikan jumlah transaksi yang tercantum sesuai dengan jumlah transaksi nasabah,
5) Simpan bukti transaksi untuk dicocokkan dengan tagihan yang nasabah terima di kemudian hari,
6) Awasi selalu gawai/device nasabah. Logout semua akun ecommerce sebelum melakukan perawatan/backup gawai dan jangan berikan userID/password kepada teknisi.
7) Konfirmasi
8) Segera hubungi Mandiri Call 14000 untuk konfirmasi apabila terjadi hal- hal sebagai berikut:
9) Kartu nasabah hilang atau dicuri. Segera lakukan blokir kartu kredit atau kartu debit melalui Livin' by Mandiri.
10) Terdapat transaksi yang tidak ketahui pada histori transaksi di LIvin' by Mandiri.
11) Terdapat notifikasi SMS / WA untuk transaksi yang tidak nasabah lakukan.
12) Terdapat tagihan yang tidak sesuai pada lembar tagihan kartu kredit nasabah.

Selain itu, Bank Mandiri juga memberikan layanan sarana kontak yang dapat dihubungi oleh nasabah diantaranya :

1) Email : mandiricare@bankmandiri.co.id
2) Mandiri Call : 14000
3) Twitter : @mandiricare
4) Facebook : @bankmandiricare

6. Bank Permata

Penipuan *social engineering* merupakan penipuan yang dapat dicegah dengan dilakukan beberapa cara. Dalam mencegah penipuan tersebut, Bank Permata memberikan sosialisasi mengenai ciri – ciri penipuan *social engineering* seperti menyamar sebagai petugas bank dengan memakai *call center* palsu memberikan undian yang berhadiah palsu, mengirimkan tautan link yang mencurigakan. Seperti pada gambar IV.11 :

Gambar IV. 10 Poster Sosialisasi Bank Permata Melalui Website

Sumber : permatabank.com

Melalui laman websitenya, Bank Permata membagikan sosialisasi mengenai jenis – jenis serangan *social engineering* seperti *phising, spear phisng, whealing, shoulder surfing, vishing, smishing,skimming.* Selain itu Bank Permata juga mensosialisasikan langkah – langkah untuk menghindari serangan phising, diantaranya :

- Jangan pernah mengirimkan informasi sensitif melalui email. Perlu diketahui, bahwa suatu perusahaan tidak akan meminta informasi sensitif melalui email atau sarana elektronis lainnya, yang tidak aman.
- Jika terlanjur membalas email/SMS dari pelaku terindikasi phishing, segera lakukan penggantian password, PIN, dan data keamanan lainnya.
- Pastikan *Reference Code/Response Code* pada pesan *One Time Password* (OTP) yang diterima sama dengan *Reference Code/Response Code* transaksi yang dituju. Hal ini terkait adanya modus *phishing* oleh *fraudster* dengan membelokkan *server* penginput kode OTP, salah satu cirinya adalah layar komputer/HP Anda berkedip.
- Menggunakan *anti virus* yang terkini.
- Jangan mengklik link apa pun pada pesan (*email*) yang terindikasi *phishing*.
- Mengkonfirmasikan kepada pihak Bank, melalui Contact Center yang resmi, jika ada permintaan yang mencurigakan.
- Jangan pernah memasukkan user ID dan password pada suatu halaman *web* yang terbuka otomatis *(pop up)* atau dari *link*. Ketiklah alamat halaman *web* yang akan dibuka.
- Hati-hati mengunduh *attachment email*, karena dapat berisi *virus/malware*, yang dapat mencuri data sensitive

Kemudian, Bank Permata memberikan sosialisasi mengenai pentingnya untuk menjaga informasi rahasia. Adapun informasi rahasia salah satunya adalah nomor –nomor penting atau keramat yang harus dijaga diantaranya OTP, CVV, PIN, nomor telepon seluler . Bank Permata juga memberikan sosialisasi bahwa Bank Permata tidak pernah meminta data atau informasi rahasian dari nasabah. Dalam rangka menjaga keamanan data rekening saat menghubungi petugas Call Center, kini Bank Permata

menggunakan teknologi Voice ID yang menggunakan suara untuk menghasilkan identifikasi unik dari setiap individu dan mempersingkat waktu proses verifikasi, sehingga kebutuhan nasabah dapat segera ditangani.

Bank Permata juga menghimbau, jika terdapat hal yang mencurigakan dan tidak wajar, maka segera untuk menghubungi layanan sarana kontak Bank Permata diantara nya :

- *Email* : care@permatabank.co.id
- PermataTel : 1500-111
- *Twitter* : @PermataCare
- *Instagram* : @permatabank
- *Facebook* : PermataBank

Berdasarkan sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh bank – bank besar di Indonesia melalui website memiki segi kebermanfaatan yang baik bagi bank sendiri dan bagi nasabah. Hal ini disebabkan media website diakses melalui jaringan internet, sehingga memudahkan nasabah untuk mengakses sosialisasi pencegahan penipuan *social engineering* dimana pun dan kapan pun. Bagi bank sendiri, penggunaan media website memudahkan bank untuk membagikan sosialisasi terkait dengan pencegahan penipuan *social engineering*, karena pembagian sosialisasi ini dapat dilakukan secara menyeluruh yaitu siapa saja dapat mengakses atau mengetahui sosialisasi tersebut.Selain itu, penggunaan website sebagai media untuk memberikan sosialisasi lebih efektif dan efisien karena tidak membutuhkan waktu yang lama untuk memberikan sosialisasi pencegahan penipuan *social engineering*.

Berdasarkan olah hasil data yang telah dijelaskan sebelumnya, sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank

Permata, Bank Syariah Indonesia (BSI) memuat informasi seperti ciri – ciri penipuan, layanan sarana kontak, dan langkah – langkah pencegahan penipuan *social engineering*. Sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh keenam bank tersebut, umumnya memberikan himbauan kepada nasabah untuk menjaga informasi data pribadi. Selain itu, keenam bank tersebut menyediakan layanan *call center* bagi nasabah yang memerlukan bantuan bank. Tidak hanya *call center* yang menjadi sarana layanan kontak, namun ada juga yang memberikan sarana kontak yang lainnya seperti email, Instagram, twitter, whatsapp seperti yang dilakukan oleh BCA. Kemudian dilanjutkan oleh BRI yang memberikan sarana kontak whatsapp, email, instagram. Selanjutnya BSI yang menyediakan layanan sarana kontaknya seperti email, instagram, twitter. Sedangkan Bank Mandiri menyediakan layanan sarana kontak seperti email dan twitter. Bank Permata menyediakan email, Instagram, twitter sebagai layanan sarana kontaknya. Dari semua layanan sarana kontak yang diberikan oleh bank – bank tersebut, sarana kontak whatsapp BRI yang paling banyak disebut di halaman websitenya dibandingkan sarana kontak milik bank – bank lainnya. Hal ini dibuktikan dengan jumlah kata yang muncul dalam point sarana kontak whatsapp yang terdapat pada tabel IV.2 yaitu 305 kata.

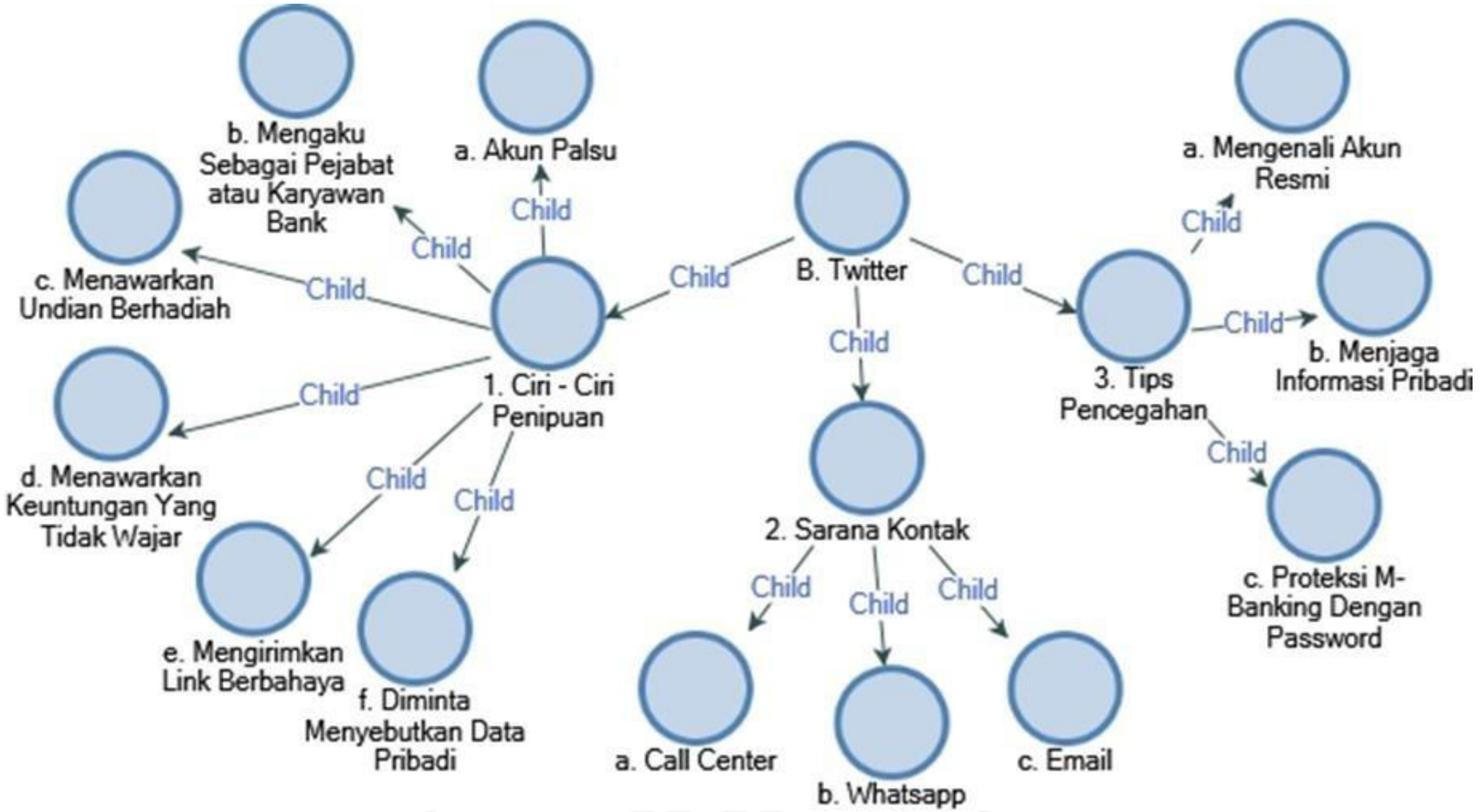
Lebih lanjut, dalam website tersebut dimuat juga informasi mengenai langkah – langkah pencegahan penipuan *social engineering.* Pada halaman website BNI memuat informasi yang lengkap mengenai langkah – langkah pencegahan penipuan *social engineering* seperti mengenali akun resmi, menghubungi *call center* resmi ketika memerlukan bantuan, menjaga informasi data pribadi, jangan mempercayai iming - iming hadiah, dan menghindari klik tautan yang mencurigakan. Namun berbeda dengan BCA yang lebih banyak mensosialisasikan mengenai langkah – langkah pencegahan penipuan, yang hal ini dibuktikan pada tabel IV.2 dengan jumlah kata yang muncul dalam halaman

web BCA yaitu 879 kata. Sosialisasi yang diberikan BCA mengenai langkah pencegahan penipuan *social engineering* lebih memfokuskan kepada mengenali akun resmi yang ditandai dengan jumlah kata yang disebut di halaman website nya yaitu 505 kata.

4.4.2 Twitter

Twitter merupakan media sosial yang memudahkan bank untuk membagikan informasi kepada pengikutnya terkait dengan kasus penipuan *sosial engineering* dan cara pencegahan nya. Bank – bank besar di Indonesia membagikan informasi tersebut dapat dalam bentuk foto, video, tautan, dan teks. Postingan twit yang dibuat oleh bank mengenai penipuan *sosial engineering* umumnya menginfokan ciri – ciri penipuan, sarana kontak, serta langkah – langkah pencegahan. Namun, terdapat perbedaan sosialisasi melalui website dan di twiiter, yaitu sosialisasi di website lebih informatif, karena website yang sifatnya halaman web yang dapat memuat informasi tanpa ada batasan kata, sedangkan twitter ketika membuat twit ada batasan 280 karakter. Oleh karena itu di twitter di dominasi informasi yang memiliki kalimat pendek. Berikut ini peneliti akan memaparkan pola – pola sosialisasi bank dalam pencegahan *sosial engineering* yang diberikan melalui twitter yang diolah peneliti menggunakan Sofware *NVivo12* yang terdapat pada gambar IV.12:

Gambar IV. 11 Peta Analisa Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Twitter*



Sumber : Diolah Peneliti Menggunakan NVivo 12

Tabel IV. 3 *Matrix Coding Query* Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Twitter* (Berdasarkan Jumlah Kata)

Pola – Pola Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui *Twitter*	BCA	BNI	BRI	BSI	Mandiri	Permata
1. Ciri - Ciri Penipuan	0	0	0	0	0	0
a. Akun Palsu	55	133	240	302	3298	17
b. Mengaku Sebagai Pejabat atau Karyawan Bank	85	446	195	329	217	43
c. Menawarkan Undian Berhadiah	0	0	0	107	0	90
d. Menawarkan Keuntungan Yang Tidak Wajar	10	0	38	0	0	49
e. Mengirimkan Link Berbahaya	0	0	74	119	123	0
f. Diminta Menyebutkan Data Pribadi	12	69	79	238	3148	323
2. Sarana Kontak	15	95	0	0	8	0
a. Call Center	15	114	116	72	109	0
b. Whatsapp	19	1192	43	0	0	0
c. Email	0	0	0	0	27	0
3. Langkah – Langkah Pencegahan	19	453	0	0	12	0
a. Mengenali Akun Resmi	67	2320	235	39	3299	17
b. Menjaga Informasi Pribadi	105	35	286	235	3315	127
c. Proteksi M-Banking Dengan Password	29	0	128	45	0	43

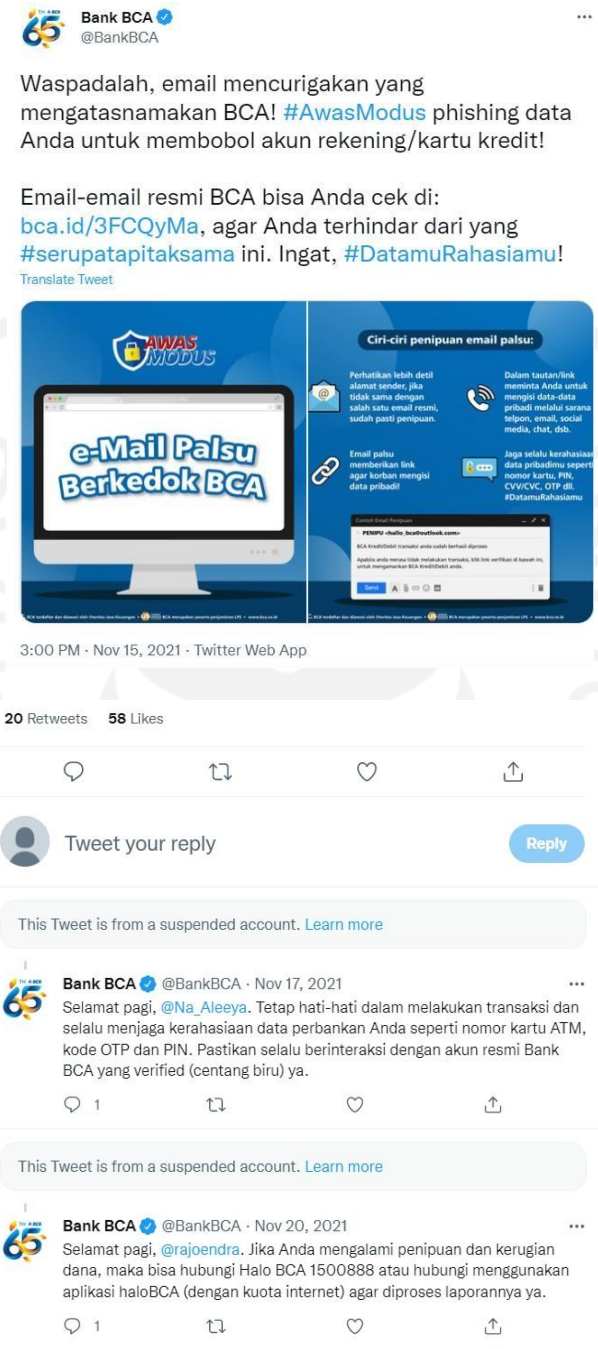
Sumber : Diolah Peneliti Menggunakan NVivo 12

Gambar IV.11 dan Tabel IV.3 merupakan informasi *coding* yang dihasilkan saat mengolah hasil data *NCapture twitter* bank resmi yang telah peneliti olah menggunakan bantuan *Software NVivo 12*. Gambar dan tabel tersebut memaparkan pola – pola strategi sosialisasi pencegahan penipuan *social engineering* menggunakan *twitter*. Adapun hasil *coding* pada tabel IV.3 memberikan keterangan "angka" yang artinya banyaknya jumlah kata – kata yang sering muncul dari poin – poin sosialisasi pencegahan penipuan *social engineering* melalui *twitter*. Lebih lanjut peneliti akan menginterpretasi hasil analisis tersebut ke dalam uraian – uraian berikut ini :

1. Bank Central Asia (BCA)

Interaksi Bank Central Asia dengan pengikutnya cukup interaktif dilihat dari twit BCA yang memention dan mereply twit dari pengikutnya untuk memberikan himbauan peringatan agar berhati – hati dengan penipuan yang mengatasnamakan BCA. Sekaligus BCA memberikan informasi mengenai ciri – ciri penipuan email palsu dan memberikan sarana kontak email resmi milik BCA. Selain sarana kontak email, Bank Central Asia (BCA) juga memberikan sarana kontak yang lainnya diantaranya *call center, dan whatsapp* yang dicantumkan saat mention pengikut nya di twitter. Sebagaimana yang terdapat dalam gambar IV.14:

Gambar IV. 13 Postingan Twit Sosialisasi Bank Central Asia (BCA)



Sumber : Twitter @BankBCA

Bank Central Asia (BCA) juga membagikan twit yang berkenaan dengan *sosialisasi engineering* yaitu memperingatkan kepada nasabah nya untuk menjaga informasi pribadi dan tidak diberikan data tersebut kepada siapa pun. BCA juga mengarahkan nasabah untuk mengenali nomor resmi *whatsapp* BCA serta

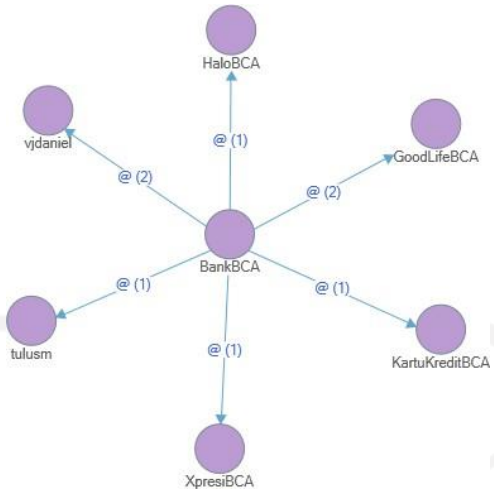
mensosialisasikan akun whatsapp yang palsu agar nasabah lebih paham dan berhati – hati terhadap modus penipuan. Sebagaimana yang terdapat dalam gambar IV.15:

Gambar IV. 14 Sosialisasi Akun Palsu Whatsapp BCA Melalui Twitter

Sumber : Twitter @BankBCA

Berdasarkan penggunaan media sosial twitter, Bank Central Asia aktif berinteraksi kepada para pengikut nya baik itu memberikan twit mengenai sosialisasi pencegahan penipuan atau informasi lainnya. Dengan demikian, peneliti akan menunjukkan aktivitas Bank Central Asia (BCA) di media sosial twitter dengan menggunakan bantuan software NVivo 12 dengan tampilan twitter sociogram :

Gambar IV. 15 Twitter Sociogram BCA



Sumber : Diolah Peneliti Menggunakan Software NVivo 12

Berdasarkan tampilan data sociogram, BCA menggandeng *public figure* tulusm dan vjdaniel untuk membantu mengkampanyekan program – program BCA. Seperti pada vjdaniel yang menjadi *brand ambassador* BCA yang menunjukkan keseruan nya menjadi CS BCA, yang memperlihatkan pelayanan yang baik kepada para nasabah nya. Hal ini menunjukkan bahwa BCA memperdulikan setiap layanan yang diberikan nasabah ketika mendapatkan masalah melalui *coustomer service* BCA.

2. Bank Mandiri

Upaya yang dilakukan oleh Bank Mandiri untuk mencegah penipuan yaitu dengan mensosialisasikan pencegahan penipuan melalui twitter dan memberikan pelayanan kepada nasabah berupa sarana layanan kontak, diantaranya :

a. Mandiri Call : 1400

b. Email : mandiricare@bankmandiri.co.id

Bank Mandiri juga menghimbau pengikutnya di twitter untuk berhati – hati kepada akun palsu yang mengatasnamakan Bank Mandiri. Selain itu, Bank Mandiri memberikan

langkah – langkah pencegahan *sosial engineering* yang di posting melalui twitter dalam bentuk video. Sebagaimana yang terdapat dalam twit nya :

Gambar IV. 16 Sosialisasi Langkah – Langkah Pencegahan *Social Engineering* Bank Mandiri Melalui Twitter

Sumber : Twitter @bankmandiri

Adapaun langkah – langkah pencegahan nya seperti :

a. Mengabaikan jika ada akun yang tidak dikenal mengatasnamakan Bank Mandiri
b. Jangan pernah mengklik tautan link, jika terdapat yang mengirimkan link di direct Message (DM) atau kolom komentar, program undian fiktif, serta *cell center* tipu – tipu,

c. Jangan pernah mengisi form untuk update data rahasia dari link yang mengatasnamakan Bank Mandiri

d. Jangan tergiur dengan program undian fiktif, Bank Mandiri selalu menginformasikan program undian melalui website dan media sosial resmi Bank Mandiri yang terverifikasi dengan centang biru dan hijau

e. Pastikan hanya menghubungi mandiri call 1400, jangan mudah terkecoh dengan call center palsu yang mengatasnamakan Bank Mandiri.

3. Bank Rakyat Indonesia (BRI)

Aktivitas Bank Rakyat Indonesia di media twitter dapat terbilang aktif karena BRI selalu mengupdate informasinya baik informasi tentang edukasi, promosi, atau layanan lainnya. BRI memiliki tiga akun twitter diantaranya @bankBRI_ID, @kontakBRI, @promo_BRI ketiga akun tersebut merupakan akun twitter yang telah terverifikasi atau bercentang biru. Ketiga akun tersebut sama – sama memberikan himbauan untuk selalu berhati – hati terhadap penipuan dan selalu menjaga kerahasiaan data seperti PIN, username, password, OTP, CVV/CVC dan lainnya. Namun, pada akun @kontakBRI lebih banyak membagikan twit mengenai langkah – langkah pencegahan penipuan dan contoh – contoh penipuan yang sering terjadi yang ditampilkan dalam bentuk poster. Informasi yang dibagikan dalam bentuk poster inilah yang menjadi hal menarik bagi pengikutnya. Seperti gambar di bawah ini :

Gambar IV. 17 Poster Langkah – Langkah Pencegahan Penipuan BRI

Sumber : Twitter @kontakBRI

Selain itu, akun instagram @kontakBRI juga memberikan sosialisasi mengenai cara untuk mengenali ciri – ciri akun palsu yang mengaku sebagai pihak BRI. Tentunya informasi ini dibagikan dengan visualisasi poster, yang hal ini dapat membuat pengguna nya menarik untuk membacanya. Kemudian, dalam poster tersebut dicantumkan juga sarana kontak yang dapat dihubungi oleh nasabah nya seperti call center, situs website, dan media sosial instagram, twitter, dan facebook. Sebagaimana yang terdapat dalam gambar berikut ini :

Gambar IV. 18 Poster Ciri – Ciri Akun Instagram Palsu BRI

Sumber : Twitter @kontakBRI

4. Bank Negara Indonesia (BNI)

Upaya pencegahan penipuan *social engineering* juga dilakukan oleh Bank Negara Indonesia. Sosialisasi yang diberikan BNI melalui dua akun twitter yaitu @BNI dan @BNICoustomerCare, tentunya kedua akun tersebut sudah terverifikasi atau sudah bercentang biru. BNI melalui akun twitternya selalu menghimbau pengikutnya untuk berwaspada pada tindakan penipuan yang mengatasnamakan BNI di twitter. Berdasarkan twitnya, BNI juga memberikan sosialisasi bahwa akun twitter BNI hanya dua yaitu @BNI dan @BNICustomerCare yang melayani pertanyaan dan keluhan nasabah. Sebagaimana twit yang diposting melalui akun twitter BNI:

Gambar IV. 19 Sosialisasi Pencegahan Penipuan Melalui Twit BNI

Sumber : twitter @BNICustomerCare

Berdasarkan postingan twit diatas, sudah di reply oleh 1.993 pengguna twitter dan di *like* 538 pengguna. Hal ini menandakan bahwa dengan postingan twit tersebut, pengguna twitter merasa bahwa informasi tersebut berguna bagi mereka dilihat dari jumlah *like* dan yang me-*reply*. Selain itu, sosialisasi yang dilakukan oleh BNI dominan dengan memberikan twit berupa text dan sering me-*reply* tanggapan yang diberikan untuk twit orang lain.

5. Bank Syariah Indonesia (BSI)

Sebagai langkah untuk mencegah penipuan *social engineering*, Bank Syariah Inonesia memberikan sosialisasi pencegahan penipuan melalui akun twitter resmi nya yaitu @bankbsi_id. Adapun sosialisasi yang diberikan BSI yaitu dapat berupa himbauan agar berhati – hati terhadap modus penipuan yang mengaku sebagai petugas BSI melalui akun palsu dan BSI juga memerintahkan pengikutnya agar segera mereport dan block akun palsu tersebut. Seperti melalui twit yang dibagikan oleh BSI pada gambar dibawah ini :

Gambar IV. 20 Sosialisasi Akun Palsu BSI

Sumber : twitter @bankbsi_id

Selain itu, akun twitter BSI juga membagikan poster mengenai ciri – ciri akun palsu melalui twitnya, hal ini merupakan sosialisasi kepada pengikut nya agar dapat mengenali akun palsu, yang diharapkan menjadi langkah pencegahan penipuan bagi pengikutnya. Sebagaimana yang terdapat dalam poster berikut ini :

Gambar IV. 21 Poster Ciri – Ciri Akun Palsu BSI

Sumber: twitter @bankbsi_id

Dalam melakukan pencegahan penipuan *social engineering*, Bank Permata sebagai Bank pilihan nasabah nya melakukan tindakan – tindakan preventif dengan memberikan sosialisasi pencegaha penipuan *social engineering* melalui akun resmi twitternya yaitu @PermataBank.

Bentuk sosialisasi Bank Permata yaitu memberikan himbauan kepada pengikutnya agar berhati – hati terhadap penipuan yang meminta data pribadi nasabah nya. Twit tersebut diselipkan pada twit yang menginformasikan pengumuman pemenang *give away* Bank Permata, sehinga secara tidak langsung pengikutnya akan tertarik untuk melihat twit tersebut, dan sudah pasti pengikutnya akan melihat kalimat himbauan agar berhati – hati terhadap penipuan. Hal ini merupakan strategi Bank Permata dalam mensosialisasikan pencegahan penipuan agar banyak pengikutnya yang mau melihat twit tersebut. Sebagaimana yang sampaikan oleh Bank Permata melalui akun twitter nya :

Gambar IV. 22 Sosialisasi Pencegahan Penipuan Bank Permata

Sumber: Twitter @PermataBank

Selain itu, Bank Permata juga memberikan sosialisasi pencegahan penipuan *social engineering* dengan poster. Poster yang dibagikan melalui twitnya, mengenai sosialisasi

ciri - ciri akun *whatsapp* palsu. Sosialisasi melalui poster ini dapat menarik perhatian pengikutnya karena dengan poster memiliki tampilan yang berwarna dan mencolok, sehingga membuat pengikutnya penasaran untuk membacanya. Sebagaimana yang terdapat dalam gambar berikut :

Gambar IV. 23 Poster Sosialisasi Pencegahan Penipuan Bank Permata

Sumber : Twitter @PermataBank

Berdasarkan sosialisasi pencegahan penipuan *social engineering* yang diberikan oleh para bank – bank diatas, dapat disimpulkan bahwa penggunaan media sosial twitter memudahkan bank untuk membagikan informasi kepada para pengikutnya terkait dengan kasus penipuan *sosial engineering* dan cara pencegahan nya. Bank – bank besar di Indonesia membagikan informasi tersebut dapat dalam bentuk foto, video, tautan, dan teks. Postingan twit yang dibuat oleh bank mengenai penipuan *sosial engineering* umumnya menginfokan ciri – ciri penipuan, sarana kontak, serta langkah – langkah pencegahan penipuan *social engineering*.

Sosialisasi pencegahan penipuan *social engineering* yang dilakukan boleh Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI) umumnya memberikan himbauan kepada nasabah untuk menjaga informasi pribadi, dan mengenali akun resmi milik Bank. Enam bank tersebut memberikan sosialisasi mengenai modus yang sering digunakan oleh pelaku yaitu pelaku mengaku sebagai petugas bank, alih – alih untuk mendapatkan perhatian dari korban.

Selain itu, ciri – ciri penipuan selanjutnya adalah pelaku penipuan sering mengirimkan link berbahaya kepada nasabah . Hal ini pun telah disosialisasikan oleh Bank BRI, BSI, dan Bank Mandiri. Sosialisasi mengenai link berbahaya ini pun lebih banyak disosialisasikan di akun twitter Bank Mandiri ditandai dengan jumlah kata yang sering muncul dalam twit – twit Bank Mandiri mengenai mengirimkan link berbahaya yaitu 123 kata.

Lebih lanjut, ciri – ciri penipuan yang lainnya adalah pelaku penipuan umumnya menawarkan keuntungan yang tidak wajar sebagai modus penipuan nya. Hal ini pun telah disosialisasikan oleh BCA, BRI, Permata. Dibandingkan dengan bank lain, BRI banyak mensosialisasikan terkait dengan modus ini yang terlihat pada jumlah kata yang sering muncul dalam twit – twit BRI mengenai modus menawarkan keuntungan yang tidak wajar yaitu 49 kata.

Adapun ciri – ciri penipuan yang terakhir adalah pelaku penipuan menggunakan modus menawarkan hadiah fiktif agar korban nya terjebak pada aksi kejahatan pelaku. Ciri – ciri penipuan ini sudah umum terjadi, maka dari itu ciri – ciri penipuan ini disosialisasikan oleh BSI dan Bank Permata sebagai upaya pencegahan penipuan *social*

engineering. Dari kedua bank ini, BSI memiliki jumlah kata yang lebih banyak dalam menyebutkan modus penipuan dengan menawarkan hadiah fiktif yaitu 107 kata.

Berdasarkan hasil olah data diatas, pada tabel IV.3 jika dilihat secara keseluruhan jumlah kata terbanyak yang menyebutkan poin – poin sosialisasi pencegahan penipuan *social engineering* adalah Bank Mandiri. Hal ini dilihat dari kotak yang bewarna biru pada tabel IV.3 yang menandakan jumlah kata yang disebut lebih banyak dibandingkan dengan bank – bank lain. Adapun poin – poin yang memiliki jumlah kata terbanyak pada Bank Mandiri yaitu ciri – ciri penipuan pada poin akun palsu memiliki 3298 kata, dan pada point diminta menyebutkan data pribadi yaitu 3148 kata. Selain itu terdapat juga pada point langkah – langkah pencegahan penipuan yang memiliki jumlah kata terbanyak yang disebutkan yaitu mengenali akun resmi yang memiliki jumlah kata 3299 kata, dan menjaga informasi pribadi 3315 kata.

4.5 Kekurangan Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* di Media Website dan Media Sosial Twitter

Berdasarkan penjelasan sebelumnya mengenai sosialisasi pencegahan penipuan *social engineering*, menurut peneliti terdapat beberapa kekurangan yang terjadi dalam sosialisasi pencegahan penipuan *social engineering* tersebut. Agar tercipta sosialisasi yang bermanfaat bagi masyarakat luas, perlu untuk sosialisasi pencegahan ini dilakukan secara optimal. Dengan demikian, untuk mengetahui perbaikan yang perlu dilakukan, peneliti terlebih dahulu memaparkan kekurangan – kekurangan yang terdapat dalam sosialisasi melalui media website dan twitter :

4.5.1 Kekurangan Pada Sosialisasi Melalui Media Website

Penggunaan website sebagai media sosialisasi merupakan cara yang tepat digunakan di zaman sekarang ini, karena dengan adanya perkembangan teknologi yang

semakin mempermudah segala aktivitas. Sosialisasi menggunakan website, dapat membagikan informasi dalam bentuk text,dan gambar. Sebagaimana yang dilakukan oleh keenam bank yaitu Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI). Namun, indikator yang menjadi pengukur bahwa sosialisasi itu bermanfaat atau tidak dilihat dari jenis informasi yang diberikan.

Adapun informasi yang diberikan oleh keenam bank tersebut mengenai sosialisasi pencegahan penipuan *social engineering*. Sosialisasi yang diberikan dapat berupa informasi apa saja yang berkaitan dengan penipuan *social engineering*. Namun, terdapat beberapa kekurangan pada sosialisasi pencegahan penipuan *social engineering* yang dibagikan oleh bank – bank tersebut melalui media website, diantaranya :

1. Bank tidak meng-*upgrade* informasi mengenai sosialisasi pencegahan penipuan, sehingga informasi yang diberikan masih dengan isu yang lama serta pencegahan nya pun masih dengan cara yang lama. Adapun bank – bank yang belum mengupgrade materi sosialisasinya dengan isu terkini diantaranya Bank Mandiri, BNI, BSI.
2. Dalam membagikan konten sosialisasi melalui website, perlu untuk menampilkan bacaan yang menarik agar nasabah semangat dalam membaca. Tidak hanya tulisan teks berwarna hitam dengan *background* website yang polos, namun sosialisasi pencegahan *social engineering* ini dapat dibagikan dalam bentuk poster yang memiliki visualisasi yang unik dan menarik seperti yang dilakukan oleh Bank Permata dan BRI.
3. Tindakan pencegahan yang dapat dilakukan pertama kali adalah mengenali apa saja ciri – ciri penipuan *social engineering* . Namun terdapat beberapa bank yang tidak memberikan sosialisasi secara lengkap mengenai ciri – ciri penipuan *social engineering* yaitu pelaku penipuan menggunakan akun palsu sebagai media

perantaranya.. Adapun bank tersebut adalah BNI, BSI, Bank Mandiri, dan Bank Permata.

4. Menjadi hal penting bagi bank – bank untuk mensosialisikan mengenai langkah – langkah pencegahan penipuan *social engineering*. Berdasarkan hasil olah data, informasi yang diberikan BCA, BRI, BSI, dan Bank Permata tidak secara lengkap memberikan langkah – langkah pencegahan yaitu menghindari untuk meng-klik tautan link yang dirasa mencurigakan, karena pada dasarnya penipuan *social engineering* dapat terjadi berawal dari pengiriman link yang berbahaya bagi nasabah. Link tersebut umumnya mengarahkan korban untuk mengisi data privasi nasabah. Sehingga diperlukan untuk mensosialisasikan terkait hal ini.
5. Dalam pemberian sosialisasi kepada nasabah perlu untuk mencantumkan sarana layanan kontak pada sosialasi pencegahan penipuan melalui website. Selain *call center*, bank perlu untuk memberikan layanan sarana kontak yang lain nya agar nasabah mudah untuk berkomunikasi dengan bank. Seperti penggunaan sarana kontak dengan yang lainnya atau menggunakan media sosial, yaitu instagram, twitter, dan email. Media sosial yang sering banyak orang gunakan untuk berkomunikasi, menjadi penting untuk bank mengikuti zaman dengan menyediakan sarana kontak dengan media sosial. Adapaun BNI yang tidak mencantumkan media sosial lainnya pada sosialisasi pencegahan penipuan dalam halaman webnya.

4.5.2 Kekurangan Pada Sosialisasi Melalui Media Twitter

Penggunaan media twitter sebagai media sosialisasi merupakan hal yang tepat dilakukan, karena banyak orang yang berinteraksi menggunakan twitter. Twitter sebagai media sosialisasi dapat dikatakan berhasil jika memberikan sosialisasi yang tepat dan dibutuhkan oleh pengikutnya.

1. Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI) umumnya memberikan sosialisasi mengenai ciri – ciri penipuan. Namun yang menjadi perhatian adalah ketika bank – bank tersebut tidak memberikan informasi yang lengkap mengenai ciri – ciri penipuan. Seperti BCA, BNI, BRI,Bank Mandiri dan Bank Permata tidak memasukan modus menawarkan undian berhadiah sebagai ciri – ciri penipuan *social engineering*.
2. Sosialisasi yang diberikan melalui twitter perlu untuk mencantumkan layanan saranan kontak yang dapat dihubungi nasabah jika nasabah memerlukan bantuan. Tidak hanya *call center* saja yang menjadi layanan sarana kontak, namun harus ada layanan kontak lainnya yang dapat diakses oleh nasabah. Berdasarkan hasil olah data, BCA, BNI, BRI, Bank Permata menyediakan sarana kontak *call center*, namun tidak menyertakan layanan sarana kontak email. Layanan sarana kontak melalui email juga tak kalah penting, karena email dapat membantu nasabah untuk mengirim dokumen yang banyak kepada Bank dan menggunakan email merupakan sebuah fleksibilitas untuk berkomunikasi dengan orang lain.
3. Dalam membagikan sosialisasi pencegahan penipuan *social engineering* melalui media twitter, tentunya tweet yang dibagikan memiliki batasan karakater yaitu 280 karakter, sehingga dalam menyampaikan informasi melalui postingan twit tidak dapat terlalu panjang, dan memberikan informasi pun harus singkat, namun isi nya tetap jelas yaitu tidak mempengaruhi kualitas informasinya. Untuk mengatasi hal tersebut, penyampaian informasi dapat menggunakan tautan gambar dan video yang isi nya mengenai penipuan *social engineering* dan langkah – langkah pencegahan nya. Selain itu, sisi positif nya penyampaian sosialisasi pencegahan penipuan *social engineering* menggunakan gambar dan video dapat menarik orang untuk membaca

karena dengan tampilan yang menarik membuat orang semangat untuk membaca. Hal ini pun telah dilakukan oleh BCA, BRI, Bank Mandiri, dan Bank Permata, para bank – bank tersebut membagikan sosialisasi yang berkaitan dengan penipuan *social engineering* dalam bentuk gambar poster atau video. Namun, pada BNI belum mengikuti strategi sosialisasi dengan membagikan poster ataupun video. BNI dalam menyampaikan sosialisasinya lebih dominan membagikan postingan tweet dengan text tanpa gambar ataupun video.

4.6 Perbaikan yang Dapat Dilakukan Bank Dalam Pencegahan Penipuan *Social Engineering*

Sosialisasi pencegahan penipuan *social engineering* melalui media website dan media twitter menjadi perhatian penting bagi nasabah yang belum memiliki pengetahuan mengenai cara pencegahan penipuan *social engineering*. Bank sebagai lembaga perantara keuangan yang dipercaya masyarakat untuk menghimpun dana dan menyimpan segala informasi rahasia yang dimiliki nasabah, memiliki kewajiban untuk memberikan sosialisasi tentang pencegahan penipuan ini. Oleh karena itu, bank harus memberikan sosialisasi yang informatif dan bermanfaat bagi nasabah nya, sehingga sosialisasi yang diberikan melalui website dan *twitter* harus tersampaikan dengan baik dan optimal kepada nasabah. Dengan demikian, dari kekurangan sosialisasi yang telah dijelaskan sebelumnya, peneliti akan merumuskan beberapa langkah perbaikan dalam melakukan sosialisasi pencegahan penipuan *social engineering* melalui media website dan media sosial yang diberikan oleh bank – bank besar di Indonesia yaitu Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Permata, Bank Syariah Indonesia (BSI).

4.6.1 Perbaikan yang Dapat Dilakukan Bank Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Media Website

Sosialisasi pencegahan penipuan *social engineering* memang sangat dibutuhkan mengingat kasus penipuan *social engineering* masih marak terjadi. Sosialisasi yang dilakukan oleh bank dapat dilakukan secara online, dan bank juga memiliki kesempatan yang banyak dengan hadirnya internet untuk membagikan sosialisasi nya melalui media online, sehingga sosialisasi tersebut dapat disampaikan secara meluas. Salah satu media yang dapat digunakan adalah media website. Namun, dari segala kebermanfaatan penggunaan website, bank – bank tidak menggunakan media website secara optimal sebagai media sosialisasi, sehingga terdapat beberapa kekurangan dalam menyampaikan sosialisasi mengenai pencegahan penipuan *social engineering.* Adapun kekurangan tersebut diantaranya:

1. Pada website bank resmi, umumnya bank membagikan materi sosialisasi pencegahan penipuan dibagian edukasi nasabah. Sosialisasi pencegahan penipuan *social engineering* yang dibagikan melalui Bank Mandiri, BNI, BSI perlu meng*update* materi sosialisasinya. Hal ini dikarenakan serangan *social engineering* tiap tahun nya memiliki jenis serangan yang berbeda – beda dan ditambah teknologi semakin berkembang yang membuat lahirnya jenis kejahatan *social engineering* semakin beragam, sehingga diperlukan juga cara – cara mencegah serangan *social engineering* dengan jenis baru.
2. Website merupakan media yang dapat membagikan gambar, video, dan text, sehingga hal ini dapat digunakan bank sebagai sarana untuk mengoptimalkan sosialisasi pencegahan *social engineering*. Oleh karena itu BCA, BNI, Bank Mandiri, BSI dapat menggunakan gambar atau video agar sosialisasi yang diberikan melalui

media website dapat menarik nasabah untuk melihat. Lebih bagusnya sosialisasi pencegahan *social engineering* dapat divisualisasikan melalui poster yang didesain dengan warna – warna menarik agar nasabah minat consumdalam membaca.

3. Sosialisasi pencegahan penipuan *sosial engineering* harus memuat berbagai informasi yang lengkap dan menggunakan kalimat bahasa yang mudah untuk dimengerti nasabah. Informasi yang lengkap mengenai pencegahan penipuan *social engineering* dapat berupa; *Pertama,* ciri – ciri penipuan *social engineering,* dengan hal ini nasabah akan mengenali seperti apa ciri – ciri penipuan untuk menjadi langkah awal sebagai pencegahan penipuan. Adapun ciri – ciri penipuan *social engineering* yang sering terjadi yaitu memakai akun palsu, tampilan website atau media sosial lainnya meniru pihak bank, mengaku sebagai pejabat atau karyawan bank, menawarkan keuntungan yang tidak wajar, diminta menyebutkan data pribadi. *Kedua,* langkah – langkah pencegahan penipuan diantara nya mengenali akun resmi, *menghubungi call center* resmi, menjaga informasi data pribadi, tidak mudah percaya dengan iming – iming hadiah, dan menghindari klik tautan yang mencurigakan.
4. Selain itu, dalam mensosialisasikan pencegahan penipuan *social engineering* perlu untuk mencantumkan layanan sarana kontak yang dapat dihubungi nasabah. Sarana kontak ini tidak hanya *call center* saja, namun perlu bagi bank memiliki cara alternatif lain agar nasabah tidak kesulitan dalam menghubungi bank, yaitu dapat mencantumkan media sosial dan email. Hal ini mengingat bahwa orang – orang di zaman sekarang lebih banyak mengakses media sosial dan email di kehidupan sehari – harinya.

4.6.2 Perbaikan yang Dapat Dilakukan Bank Dalam Sosialisasi Pencegahan Penipuan *Social Engineering* Melalui Media Twitter

Berdasarkan kekurangan yang telah peneliti uraikan sebelumnya, bahwa perbaikan sosialisasi pencegahan penipuan melalui media sosial twitter perlu untuk dioptimalkan agar penyampaian sosialisasi pencegahan *social engineering* dapat berguna bagi nasabah bank maupun pengikut akun twitter bank tersebut. Sosialisasi pencegahan penipuan *social engineering* melalui twitter dapa berguna bagi pembaca, ketika informasi yang disampaikan jelas, singkat namun informatif, sehingga hal ini perlu diperhatikan bagi bank – bank agar sosialisasi yang diberikan berhasil. Adapun perbaikan yang perlu dilakukan oleh bank – bank tersebut diantaranya :

1. Dalam memberikan sosialiasi pencegahan penipuan *social engineering*, perlu untuk memberikan informasi yang jelas dan lengkap. Seperti hal nya, informasi mengenai mengenal ciri – ciri penipuan. Informasi mengenai ciri – ciri penipuan ini sangat penting, karena dengan mengenali ciri – ciri penipuan dapat menjadi langkah awal untuk mencegah terjadinya penipuan, sehingga sangat perlu untuk memaparkan secara lengkap ciri – ciri penipuan yang sering terjadi. Seperti modus penipuan dengan menawarkan undian berhadiah, hal ini sering terjadi, karena dengan modus seperti ini yang berhasil menaklukan korban agar korban mau menyerahakan informasi pribadi ke pelaku.
2. Penting untuk mencantumkan layanan sarana kontak pada postingan twit mengenai sosialisasi pencegahan penipuan *social engineering.* Bank – bank perlu memiliki berbagai macam sarana kontak tidak hanya *call center* saja, namun dapat mencantumkan juga alamat email bank. Layanan sarana kontak melalui email juga tak kalah penting, karena email dapat membantu nasabah untuk mengirim dokumen

dengan jumlah banyak atau bahkan sekedar memberikan laporan keluhan kepada bank.

3. Media sosial twitter merupakan layanan yang memudahkan dalam berkomunikasi melalui pertukaran pesan yang cepat dan dengan kalimat yang tidak terlalu panjang yaitu maksimal 280 karakter saja. Walaupun demikian, media sosial twitter masih dapat membagikan foto, video, tautan, dan teks. Oleh karena itu, sosialisasi yang diberikan melalui media sosial twitter tidak boleh terlalu panjang, dan harus memuat informasi yang lengkap agar dapat dibutuhkan pengikut di twitter. Selain itu, bank – bank juga dapat membagikan poster yang isi nya mengenai pencegahan penipuan *social engineering*, poster tersebut di desain semenarik mungkin agar pengikut berminat untuk membaca.

BAB V

KESIMPULAN

5.1 Pengenalan Bab

Pada bab ini menjelaskan kesimpulan atas penelitian yang telah dilakukan oleh peneliti berdasararkan rumusan masalah yang telah dibuat diawal penelitian dan disertakan juga kekurangan selama penelitian berlangusng serta saran untuk penelitian selanjutnya.

5.2 Kesimpulan

Social engineering merupakan salah satu serangan psikologis yang menyerang manusia dengan cara mengeksploitasi kelemahan atau dengan menglabui korban nya. Manusia yang memiliki sifat ceroboh, malas, dan memiliki antusiasme yang tinggi sangat mudah untuk dimanupulasi dalam memberikan informasi rahasia disalahgunakan oleh pelaku penipuan. Walaupun sistem komputer telah diberikan pengamanan dan di lindungi dengan piranti keras dan lunak yang canggih, namun jika manusia yang lalai dalam mengoperasikannya, maka peralatan tersebut tidak dapat berguna sepenuhnya. Oleh karena itu, diperlukan kesadaran dari manusia itu sendiri untuk memahami bagaimana ciri – ciri penipuan, langkah – langkah pencegahan agar terhindar dari penipuan *social engineering*. Dengan demikian, posisi bank – bank di Indonesia sebagai elemen *controller* memiliki peran penting untuk mengatasi masalah penipuan yang dialami oleh nasabah bank, yaitu dengan memberikan sosialisasi mengenai pencegahan modus *social engineering* pada nasabah bank melalui media website dan media sosial twitter. Pemberian sosialisasi ini dapat mengurangi unsur *gullibility* pada nasabah, karena dapat memperkuat cara berfikir (*cognition*) nasabah dengan bertambahnya pengetahuan mengenai modus *social engineering* dan nasabah tidak mudah terjebak dalam unsur *situation* yang telah di rancangan oleh pelaku.

Berdasarkan hasil olah data, keenam bank ini memiliki pola sosialisasi pencegahan penipuan yang berbeda – beda di setiap media yang digunakan. Sosialisasi yang dibagikan oleh BRI melalui media website lebih banyak memberikan informasi mengenai ciri – ciri penipuan *social engineering* dan layanan sarana kontak. Sementara BCA lebih banyak memberikan sosialisasi mengenai langkah – langkah pencegahan penipuan dengan mengenali akun resmi milik bank. Selanjutnya, bank yang aktif dalam memberikan sosialisasi terkait dengan pencegahan penipuan *social engineering* melalui media twitter adalah Bank Mandiri. Bank Mandiri lebih banyak memberikan sosialisasi mengenai akun palsu dan langkah – langkah pencegahan *social engineering,* serta memiliki keaktifan dalam membuat twit dan me-*reply* laporan nasabah mengenai penipuan *social engineering* serta me-*mention* akun palsu untuk di sosialisasikan kepada *followers*-nya sebagai upaya pencegahan penipuan *social engineering*. Selain itu, sosialisasi mengenai layanan sarana kontak melalui media twitter lebih banyak diberikan oleh BNI, yang banyak menyebutkan layanan sarana kontak whatsapp dalam postingan twitnya.

Optimalisasi sosialisasi melalui website dan twitter dapat dilakukan dengan cara membuat konten yang memuat informasi secara lengkap dan terkini mengenai ciri – ciri penipuan, sarana layanan kontak, dan langkah – langkah pencegahan yang dapat divisualisasikan dalam bentuk video atau gambar poster yang di desain dengan menarik agar nasabah minat dalam membaca. Langkah pencegahan yang dioptimalisasikan melalui cara ini, memudahkan nasabah untuk memahami sosialisasi mengenai modus *social engineering,* sehingga sosialisasi tersebut dapat diterima dengan baik oleh nasabah sebagai pembaca.

5.3 Keterbatasan Penelitian

Pada penelitian ini, peneliti menyadari bahwa penelitian yang dilakukan masih jauh

dari kata sempurna, walaupun dalam penelitian sudah dilakukan usaha yang maksimal. Oleh karena itu, peneliti memiliki keterbatasan yang dialami selama penelitian berlangsung yaitu pengambilan data terkait dengan sosialisasi pencegahan *social engineering* yang hanya dapat mengambil data dari media website dan media sosial twitter bank. Sementara itu, banyak sosialisasi yang diberikan oleh bank seperti melalui media facebook, instagram dan youtube. Hal ini terkendala karena tidak mendapatkan akses oleh facebook, instagram dan youtube untuk meng-*capture* konten menggunakan Software *NVivo 12*. Dengan demikian, peneliti ini masih membutuhkan kajian yang lebih dalam terkait dengan sosialisasi pencegahan penipuan *social engineering* di sektor perbankan.

5.4 Saran

5.4.1 Bank Mandiri, Bank Central Asia (BCA) , Bank Rakyat Indonesia (BRI) , Bank Negara Indonesia (BNI), Bank Syariah Indonesia (BSI), Bank Permata

Berdasarkan penelitian yang dilakukan dengan melihat kekurangan yang terjadi, maka penulis menyarankan kepada bank – bank tersebut untuk mengoptimalkan sosialisasi pencegahan penipuan *social engineering* melalui website dan twitter baik dari segi tampilan gambar poster dan video serta memberikan informasi yang jelas dan lengkap. Misalnya sosialisasi yang diberikan dalam bentuk gambar poster atau video selain ditampilkan dengan warna dan ilustarasi yang menarik, namun harus menjelaskan juga informasi yang lengkap mengenai ciri – ciri penipuan yang umum terjadi, langkah – langkah pencegahan serta sarana kontak yang dapat dihubungi oleh nasabah jika hendak membutuhkan bantuan bank. Selain itu, bank juga dapat menggandeng *public figure* atau bahkan tokoh terkenal yang menjadi idola masyarakat untuk membantu mengkampanyekan mengenai pencegahan penipuan *social engineering*, karena dengan

cara ini memungkinkan dapat menarik perhatian masyarakat agar lebih perhatian dengan modus penipuan *social engineering.*

5.4.2 Masyarakat

Dalam pencegahan penipuan *social engineering* ini, sangat diperlukan peran masyarakat untuk berwaspada, teliti, dan berhati – hati dalam menerima telepon orang yang tidak dikenal atau yang mengaku sebagai pegawai bank yang memberikan ajakan untuk memberikan informasi pribadi, dan mengiming – iming hadiah atau keuntungan yang tidak wajar, karena bank resmi tidak mungkin meminta informasi pribadi nasabah yang sifatnya rahasia. Jika ada masyarakat yang mengalami hal tersebut, segera untuk mengkonfirmasi dengan pihak bank resmi atau segera melaporkan ke pihak kepolisian jika masyarakat sudah menjadi korban penipuan *social engineering*. Bagi masyarakat yang sudah menjadi korban penipuan *social engineering* tidak perlu sungkan, malu, takut, dan merasa khawatir ketika ingin mengadukan kasus penipuan ini ke pihak kepolisian. Segera melaporkan kasus penipuan tersebut dengan membawa bukti keterangan yang memadai atas tindakan penipuan yang terjadi, sehingga mempermudah pihak kepolisian untuk melakukan penyidikan.

5.4.3 Penelitian Selanjutnya

Harapan penulis untuk peneliti selanjutnya yaitu dapat melakukan penelitian lebih lanjut mengenai sosialisasi pencegahan penipuan *social engineering* yang dilakukan oleh bank melalui media sosial yang sering digunakan oleh masyarakat seperti melalui media facebook, youtube, instagram, telegram, whatsapp, tiktok dan lain – lain,

DAFTAR PUSTAKA

Abass, I. A. M. (2018). Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Abe, N., & Soltys, M. (2019). Deploying Health Campaign Strategies To Defend Against Social Engineering Threats. *Procedia Computer Science*, *159*, 824–831. https://doi.org/10.1016/j.procs.2019.09.241

Aditama, R. (2021). Penegakan Hukum Cyber Crime Terhadap Tindak Pidana Pencurian Uang Nasabah Dengan Cara Pembajakan Akun Internet Banking Lewat Media Sosial. *Wajah Hukum*, *5*(1), 118. https://doi.org/10.33087/wjh.v5i1.360

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, *20*(2), 150–161. https://doi.org/10.1108/FS-08-2017-0043

Ahmadian, H., & Sabri, A. (2021). Teknik Penyerangan Phising Pada Social Engineering Menggunakan Set dan Pecegahannya. *Journal of Information Technology Research*, *2*, *No.1*.

Airehrour, D., Nair, N. V., & Madanian, S. (2018). Social Engineering Attacks And Countermeasures In The New Zealand Banking System: Advancing A User-Reflective Mitigation Model. *Information (Switzerland)*, *9*(5). https://doi.org/10.3390/info9050110

Ali, L. (2019). Cyber Crimes A Constant Threat For Business Sectors and Its Growth (A Study Of The Online Banking Sectors in GCC). *The Journal of Developing Areas*, *53*.

Alrashed, T., & Awadallah, A. H. (2018). *The Lifetime of Email Messages: A Large-Scale Analysis of Email Revisitation*.

Anderson, K. (2011). *Consumer Fraud in the United States, 2011 The Third FTC Survey* (3rd ed.).

Badan Siber dan Sandi Negara. (2020). *Rekap Serangan Siber (Januari – April 2020)*. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Balzer, C., Oktavian, R., Zandi, M., Fairen-Jimenez, D., & Moghadam, P. Z. (2020). Wiz: A Web-Based Tool for Interactive Visualization of Big Data. *Patterns*, *1*(8), 100107. https://doi.org/10.1016/j.patter.2020.100107

Bank Indonesia. (2021). *Jumlah Uang Elektronik Beredar*. https://www.bi.go.id/id/statistik/ekonomi-keuangan/ssp/uang-elektronik-jumlah.aspx

Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers and Electrical Engineering*, *96*(PA), 107546. https://doi.org/10.1016/j.compeleceng.2021.107546

Buist, E., Chan, W., & L'Ecuter, P. (2008). Speeding Up Call Center Simulation and Optimization by Markov Chain Uniformization. *Winter Simulation Conference*.

Cahyolaksono, B. A., Mahardhika, A., & Zakaria, M. I. (2021). Usulan kebijakan pencegahan risiko perbankan di era digital. *Entrepreneurship Bisnis Manajemen Akuntansi (E-BISMA)*, *2*(1), 18–26. https://doi.org/10.37631/e-bisma.v2i1.301

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*(2021), 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. *CONF-IRM 2019 Proceedings*, *11*, 1–9. https://aisel.aisnet.org/confirm2019/11

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design* (3rd ed.). SAGE Publication, Inc.

Dewi, P. D. R., & Darma, G. S. (2022). Menakar Efektivitas Digital Marketing Via Instagram. *Jurnal Ilmiah Edunomika*, *6*, *No.1*.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity.

Journal of Information Policy, *9*(May 2021), 280–306.

Eck, J. (2003). Police Problems: The Complexity Of Problem Theory, Research And Evaluation. *Crime Prevention Studies*, *15*, 79–113.

Enrick, M. (2019). *Pembobolan ATM Menggunakan Teknik Skimming Kaitanya Dengan Pengajuan Restitusi*. *2*(2), 555–580.

Fadhilah, A. (2019). ATM CRIME : Pengaruh Reputasi Bank & Penanganan Masalah Terhadap Loyalitas Nasabah Dengan Kepuasan Sebagai Variabel Moderating Pada Bank BRI Kediri Bagian Selatan-Jawa Timur Pasca Kasus Skimming ATM. *At-Tamwil: Kajian Ekonomi Syariah*, *1*(1), 1–16.

Gangwani, M. (2021). Suitability Of Forensic Accounting In Uncovering Bank Frauds In India: An Opinion Survey. *Journal of Financial Crime, Vol. 28 No*. https://doi.org/10.1108/JFC-07-2020-0126

Gibbs, T. (2020). Seeking Economic Cyber Security: A Middle Eastern Example. *Journal of Money Laundering Control*, *23*(2), 493–507. https://doi.org/10.1108/JMLC-09-2019-0076

Greenspan, S. (2008). *Annal of Gullibility: Why We Get Duped and How to Avoid It: Why We Get Duped and How to Avoid It.* Santa Barbara, CA: ABC-CLIO.

Hancock, D. R., & Algozzine, B. (2006). *Doing Case Study Research : A practical Guide For Beginning Researchers*. Teachers College.

Hasan, A., & Febriany, L. (2021). Identifikasi Tindakan Pengawasan Dan Pencegahan Terhadap Kejahatan Finansial Perbankan Syariah Selama Masa Pandemi COVID 19. *Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(4), 1089–1090. https://doi.org/26222191

Hasanah, U., Handoyo, A. H., Ruliana, P., & Irwansyah. (2018). Efektivitas E-mail Sebagai Media Komunikasi Internal Terhadap Kepuasan Komunikasi Karyawan. *Jurnal Komunikasi*, *3*.

Hikmatulloh, R., & Nurmiati, E. (2020). Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek).

Kosmik Hukum, *20*(2), 121. https://doi.org/10.30595/kosmikhukum.v20i2.6449

Hootsuite and We are Social. (2021). Digital 2021. *Global Digital Insights*, 103.

Iryanti, Y. S., & Rahman, M. A. (2019). Promosi Perpustakaan Melalui Media Sosial Twitter Di Perpustakaan Hukum Daniel S. Lev. *Edulib*, *9*(2), 128–143. https://doi.org/10.17509/edulib.v9i2.17763

Kartika Dewi, R. (2020, October 18). Kasus Pembobolan Rekening Rp. 400 Juta, Ini yang perlu Diwaspadai. *Kompas.Com*. https://www.kompas.com/tren/read/2020/10/18/094329565/kasus-pembobolan-rekening-rp-400-juta-ini-modus-yang-perlu-diwaspadai?page=all

Kävrestad, J. (2018). Fundamentals of Digital Forensics. In *Fundamentals of Digital Forensics* (Second). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-96319-8

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Online banking and privacy: redesigning sales strategy through social exchange. *International Journal of Bank Marketing*, *39*(6), 955–983. https://doi.org/10.1108/IJBM-05-2020-0278

Malik, M. S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, *26*(1), 50–60. https://doi.org/10.1108/JFC-11-2017-0118

Namahoot, K. S., & Laohavichien, T. (2018). Assessing The Intentions To Use Internet Banking: The Role Of Perceived Risk And Trust As Mediating Factors. *International Journal of Bank Marketing*, *36*(2), 256–276. https://doi.org/10.1108/IJBM-11-2016-0159

Olowookere, T. A., & Adewale, O. S. (2020). A Framefork For Detecting Credit Card Fraud With Cost-Sensitive Meta-Learning Ensemble Approach. *Scientific African*.

Pan, W., Liu, D., & Fang, J. (2021). An Examination of Factors Contributing to the Acceptance of Online Health Misinformation. *Frontiers in Psychology*, *12*(March), 1–11. https://doi.org/10.3389/fpsyg.2021.630268

Pustikayasa, I. M. (2019). Group Whatsapp Sebagai Media Pembelajaran. *Jurnal Ilmiah*

Pendidikan, *10*. https://doi.org/10.36417/widyagenitri.v10i2.281

Putra, D. N. P. (2011). *Research and Development Penelitian dan Pengembangan : Suatu Pengantar* (1st ed.). PT. Raja Grafindo Persada.

Ratnamulyani, Ike Atikah Maksudi, B. I. (2018). Peran Media Sosial Dalam Peningkatan Partisipasi Pemilih Pemula Dikalangan Pelajar Di Kabupaten Bogor. *Jurnal Ilmu - Ilmu Sosial Dan Humaniora*, *20*(2), 154–161. https://doi.org/1411 - 0903

Ratulangi, C. H., Wahongan, D. A. S., & Mewengkang, F. R. (2021). Tindak Pidana Vyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *IX*(5).

Richter, E., Carpenter, J. P., Meyer, A., & Richter, D. (2022). Instagram as a Platform for Teacher Collaboration and Digital. *Computer and Education*.

Rodríguez, M., Feng, A. T., Menjivar, C., López Saca, M., Centeno, C., & Arantzamendi, M. (2022). Whatsapp as a Facilitator of Expressions of Gratitude for Palliative Care Professionals. *SSRN Electronic Journal*, *166*(July). https://doi.org/10.2139/ssrn.4030474

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*, 21–26. http://jifti.upnjatim.ac.id/index.php/jifti/article/view/26

Saskara, K., & Arthani, N. L. G. Y. (2021). Tinjauan Kriminologi Terhadap Kejahatan Skimming Melalui ATM di Polda Bali. *Jurnal Mahasiswa Hukum Saraswati*, *1*(1), 125.

Saunders; Lewis; Thornhill. (2012). Research Methods For Business Students. In *International Journal of the History of Sport* (Vol. 30, Issue 1).

Shah, A., & Ravi, S. (2012). *A to Z of Cyber Crime*. Lexcode Education & Assessment Platform (LEAP).

Shelley, M., & Krippendorff, K. (1984). Content Analysis: An Introduction To Its Methodology. In *Journal of the American Statistical Association* (Vol. 79, Issue

385). https://doi.org/10.2307/2288384

Silverman, D. (2013). *Doing Qualitative Research* (Fourth). SAGE Publication, Inc.

Software Engineering Institute. (2014). *Unintentional Insider Threats: Social Engineering*. Carnegie Mellon University.

Steinebach, M., Zenglein, S., & Brandl, K. (2021). Phishing Detection On Tor Hidden Services. *Forensic Science International: Digital Investigation*, *36*, 301117. https://doi.org/10.1016/j.fsidi.2021.301117

Subiyanto, A., & Suwarto. (2007). *Metode dan Teknik Penelitian Sosial* (1st ed.). CV. Andi Offset.

Titus, R. M., Gover, A. R. (2001). Personal Fraud: The Victims And The Scams. *Crime Prevention Studies*, *12*, 133–151.

Tracy, S. J. . (2013). *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact* (1st ed.). John Wiley & Sons, Ltd.,. https://doi.org/10.5613/rzs.43.1.6

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Wall, D. S. (2017). Towards A Conceptualisation Of Cloud (Cyber) Crime. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10292 LNCS*(July), 529–538. https://doi.org/10.1007/978-3-319-58460-7_37

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Weller, K., Bruns, A., Burgess, J., Mahrt, M., & Puschmann, C. (2014). Twitter and Society. *The Journal of Media Innovations*, *1*(1), 134–137. https://doi.org/10.5617/jmi.v1i1.825