# IMPLEMENTASI PENCEGAHAN DAN PENYELESAIAN *SOCIAL ENGINEERING CUSTOMER SERVICE* PADA BANK BRI UNIT ITN II MALANG

**Claudinar Tasya Salsabil[1], San Rudiyanto[2]**

[1]Fakultas Vokasi Universitas Brawijaya, Jl. Veteran 12-16 Malang 65145
sanrudiyanto@ub.ac.id

[2]Fakultas Vokasi Universitas Brawijaya, Jl. Veteran 12-16 Malang 65145
claudinarts2121@student.ub.ac.id

**Diterima: 28 September 2023** **Layak Terbit: 4 Februari 2024**

***Abstract: Implementation of Prevention and Resolution of Social Engineering Customer Service at Bank BRI Unit ITN II Malang.*** *The development of information technology has made banking institutions change their business strategies by placing technology as the main element in the product and service innovation process. The technological sophistication applied by banking institutions has been recognized as being able to ward off potential banking crimes committed by hackers. Realizing the increasingly sophisticated protection of banking systems, hackers not only operate behind computers to attack their targets, they also approach their targets directly to obtain the valuable information they need so they can access systems protected by security fortifications and make any security measures useless. This is what is usually referred to as Social Engineering. In social engineering, the perpetrator takes advantage of human nature. This means that human nature can be known and studied and also utilized for certain purposes.*

*Social engineering crimes are very dangerous for the banking business because they have the potential to cause financial, reputational and legal losses for banks and their customers through physical attacks and psychological attacks. To reduce these risks, banks need to train and educate their staff about security threats and how to recognize and anticipate social engineering attacks. To prevent the impact of social engineering on the banking business, anticipatory steps are needed through preventing password leaks, securing information access, contact verification, following procedures, reporting suspicious actions, maintaining emotions, continuous training and providing education to customers.*

***Keywords****: Banking, Hackers, Social Engineering, Security, Information, Customers*

**Abstrak: Implementasi Pencegahan Dan Penyelesaian *Social Engineering Customer Service* Pada Bank BRI Unit ITN II Malang.** Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Kecanggihan teknologi yang

diterapkan oleh institusi perbankan telah diakui mampu menangkal potensi kejahatan perbankan yang dilakukan oleh *hacker*. Menyadari semakin canggihnya perlindungan sistem perbankan, *hacker* tidak hanya beroperasi di balik komputer untuk menyerang targetnya, mereka juga menghampiri targetnya secara langsung untuk mendapatkan informasi berharga yang mereka butuhkan sehingga dapat mengakses sistem yang terlindungi oleh benteng keamanan dan membuat penanganan keamanan apapun menjadi tidak berguna, cara seperti inilah yang biasa disebut sebagai *Social Engineering*. Dalam *social engineering*, si pelaku memanfaatkan sifat alamiah dari manusia. Hal ini diartikan bahwa betapa sifat alami manusia dapat diketahui dan dipelajari juga dimanfaatkan untuk tujuan tertentu.

Kejahatan *social engineering* sangat membahayakan bisnis perbankan karena berpotensi menimbulkan kerugian finansial, reputasi dan hukum bagi bank dan nasabahnya melalui serangan fisik dan serangan psikologis. Untuk mengurangi resiko tersebut, bank perlu untuk melatih dan mendidik staf mereka mengenai ancaman keamanan dan bagaimana caranya mengenali dan mengantisipasi serangan *Social Engineering*. Untuk mencegah dampak *social engineering* pada bisnis perbankan diperlukan langkah antisipatif melalui mencegah kebocoran password, keamanan akses informasi, verifikasi kontak, mengikuti prosedur, pelaporan tindakan mencurigakan, menjaga emosi, pelatihan berkelanjutan dan memberikan edukasi kepada nasabah.

**Kata kunci** *:* Perbankan, Hacker, Social Engineering, Keamanan, Informasi,Nasabah.

## PENDAHULUAN

Bank bagi masyarakat yang hidup di negara-negara maju, seperti negara- negara di Eropa, Amerika, dan Jepang sudah merupakan suatu kebutuhan dasar yang harus dipenuhi. Bank merupakan mitra dalam rangka memenuhi semua kebutuhan keuangan mereka sehari-hari. Bank dijadikan sebagai tempat untuk melakukan berbagai transaksi yang berhubungan dengan keuangan seperti tempat mengamankan uang, melakukan investasi, pengiriman uang, melakukan pembayaran , atau melakukan penagihan.

Masa depan industri keuangan dan perbankan berada di era digital ekonomi. Seiring dengan adanya kecanggihan teknologi membuat pendapatan profit meningkat dalam setiap perusahaan atau individu. Perubahan perilaku nasabah yang lebih menyukai transaksi digital membuat bisnis lebih cepat, aman dan juga hemat, serta para nasabah

yang menginginkan transaksi tanpa dibatasi jarak maupun waktu. Dengan demikian teknologi digital merupakan sarana yang menjajikan untuk mempermudah setiap aktivitas kehidupan manusia dalam segela bidang khususnya di bidang perbankan yang menghindari ancaman adanya tren penurunan keuntungan atau kehawatiran-kehawatiran yang menjadi dilema perbankan.

Perkembangan ilmu pengetahuan dan teknologi pada tahun terakhir ini telah menghadirkan suatu media baru *(new media)* yang memberikan banyak manfaat dan perkembanganya sangat cepat sehingga dapat membentuk kebiasaan baru dalam masyarakat. Dikutip dari (Indonesia, 2022) PT Bank Rakyat Indonesia (Persero) Tbk (BBRI) mencatat transaksi nasabah BRI bergeser ke arah digital dengan pesat. Direktur Digital dan Teknologi Informasi BRI Arga M. Nugraha mengungkapkan saat ini, sebanyak 96,7% aktivitas nasabah telah menggunakan *digital channel*. Sementara 3,3% sisanya masih datang ke unitkerja.

Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Direktur Digital dan Teknologi Informasi Bank BRI (Nugraha, 2022) menjelaskan pengguna aplikasi digital banking BRImo sepanjang 2021 tercatat tumbuh 56,4% menjadi 14,2 juta dari 9,1 juta pada 2020. Adapun jumlah transaksi juga meningkat sekitar 66,2% menjadi 1,27 miliar pada 2021 dari 766 juta transaksi pada 2020. Sementara nilai transaksi yang dibukukan melalui platform BRImo pada 2021 mencapai Rp1.345 triliun atau meningkat 581,1% dari Rp197 triliun pada 2020.

Menyadari semakin canggihnya perlindungan sistem perbankan, *hacker* tidak hanya beroperasi di balik komputer untuk menyerang targetnya, mereka juga

menghampiri targetnya secara langsung untuk mendapatkan informasi berharga yang mereka butuhkan sehingga dapat mengakses sistem yang terlindungi oleh benteng keamanan dan membuat penanganan keamanan apapun menjadi tidak berguna, cara seperti inilah yang biasa disebut sebagai *Social Engineering*.

*Social engineering* adalah teknik yang digunakan untuk mertas pengamanan akun seseorang untuk tujuan memanipulasi serta mengeksploitasi akun tersebut sesuai keinginannya. Pelaku *social engineering* menggunakan teknik rekayasa sosial untuk menyembunyikan identitas dan berpura-pura sebagau individu yang terpercaya. Kejahatan *social engineering* sangat membahayakan bisnis perbankan karena berpotensi menimbulkan kerugian finansial, reputasi dan hukum bagi bank dan nasabahnya melalui serangan fisik dan serangan psikologis. Tujuan dari *Social Engineering* sendiri sama seperti hacker hacker lainnya, yaitu untuk mendapatkan akases ke dalam sebuah sistem (Rafizan, 2019).

Kehadiran *internet banking* BRI atau sering disebut BRIMO memberi kemudahan pada nasabah dalam bertransaksi melalui aplikasi. Di dalam akun BRIMO, nasabah menyertakan beberapa informasi yang bersifat pribadi dan rahasia seperti *username*, *password*, dan PIN BRIMO. Pelaku *social engineering* juga mejadikan kartu ATM sebagai sasarannya dikarenakan dalam kartu ATM ada beberapa informasi yang bersifat rahasia sepeerti nomor kartu ATM, tanggal kadaluarsa kartu, dan juga kode yang terlampir di kartu ATM. Dalam kasus ini pelaku memanipulasi nasabah dengan berpura-pura menjadi pegawai Bank BRI dan meminta informasi nasabah yang bersifat pribadi dengan modus saat ini yaitu tarif transfer antar bank dengan sekali tranfer sebesar Rp. 6.500 menjadi Rp.

150.000 per bulan. Pelaku meminta nasabah untuk membuka dan mengisi link yang telah dikirimkan tersebut. Bagi nasabah yang awam mengenai modus penipuan akan percaya dan mengikuti anjuran dari penipu. Untuk mencegah dampak *social engineering* pada bisnis perbankan diperlukan langkah antisipatif melalui mencegah kebocoran *password*, keamanan akses informasi, verifikasi kontak, mengikuti prosedur, pelaporan tindakan mencurigakan, menjaga emosi, pelatihan berkelanjutan dan memberikan edukasi kepada nasabah.

## METODE

Metode penelitian yang digunakan oleh peneliti dalam penelitian ini adalah metode kualitatif. Menurut Creswell (2016) penelitian kualitatif adalah jenis penelitian yang mengeksplorasi dan memahami makna di sejumlah individu atau sekelompok orang yang berasal dari masalah sosial. Penelitian kualitatif secara umum dapat digunakan untuk penelitian tentang kehidupan masyarakat, sejarah, tingkah laku, konsep atau fenomena, masalah sosial, dan lain-lain. Salah satu alasan mengapa menggunakan pendekatan kualitatif adalah pengalaman peneliti dimana metode ini dapat menemukan dan memahami apa yang tersembunyi dibalik fenomena yang kadangkala merupakan suatu yang sulit untukdipahami (Bungin, 2005).

Jenis penelitian ini adalah penelitian lapangan *(field research)*. Penelitian lapangan yaitu suatu penelitian yang dilakukan di lapangan atau di lokasi untuk menyelidiki gejala objektif sebagai terjadi di lokasi tersebut, yang digunakan untuk penyusunan laporan ilmiah (Muhammad, 2008). Adapun maksud dari *field research* dalam penelitian ini adalah peneliti akan melakukan penelitian yang ditujukan secara langsung ke lokasi penelitian yang akan diteliti yaitu Bank BRI Unit ITN II Malang.

Penelitian ini bersifat deskriptif, penelitian deskriptif adalah penelitian yang bertujuan untuk menggambarkan, meringkaskan berbagai kondisi, berbagai situasi atau berbagai variabel yang timbul di masyarakat yang menjadi objek penelitian itu, kemudian menarik kepermukaan sebagai suatu ciri atau gambaran tentang kondisi tertentu. Penelitian deskriptif adalah suatu bentuk penelitian yang ditujukan untuk mendeskripsikan atau menggambarkan fenomena-fenomena yang ada, baik fenomena alamiah maupun rekayasa manusia (Moloeng, 2000).

## HASIL DAN PEMBAHASAN

Bank Rakyat Indonesia didirikan di Purwokerto oleh Raden Aria Wiriatmaja dengan nama *De Poerwokertosche Hulpen Spaarbank der Indlandsche Hoofden*, yang pada awalnya adalah lembaga yang mengelola dana kas masjid untuk disalurkan kepada masyarakat dengan skema yang sangat sederhana. Berdasarkan Undang-Undang No. 21 Tahun 1968, Pemerintah menetapkan kembali nama Bank Rakyat Indonesia sebagai Bank Umum. Bank BRI berubah status hukum menjadi PT. Bank Rakyat Indonesia (Persero) berdasarkan Undang-Undang Perbankan No.7 tahun 1992. Bank BRI menjadi Perseroan Terbuka pada tanggal 10 November 2003 dengan mencatatkan sahamnya di Bursa Efek Jakarta, kini Bursa Efek Indonesia, dengan kode saham BBRI. Sebuah langkah strategis dengan mengakuisisi Bank Jasa Artha (BJA) pada tahun 2007, yang kemudian dikonversi menjadi PT. Bank Syariah BRI. Unit Usaha Syariah BRI kemudian dipisahkan (spin off) dari Bank BRI dan digabungkan ke dalam PT. Bank Syariah BRI pada 1 Januari 2009.

### Kasus Social Engineering Bank BRI Unit ITN II Malang

Perkembangan teknologi informasi membuat industri perbankan mengubah



*VOK@SINDO Edisi Volume 12 No.1 Februari 2024*
*ISSN : 2338-5103*
*E-ISSN: 2527-340x*

strategi bisnisnya dengan menjadikan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Seperti halnya pelayanan pada Bank BRI Unit ITN II Malang melalui mesin ATM, BRIMO dan *Internet Banking* yang merupakan bentuk perubahan pelayanan transaksi manual menjadi pelayanan transaksi yang berbasis teknologi. Faktor kepercayaan dan efisiensi serta kualitas layanan menjadi alasan bagi industri perbankan untuk selalu memperbarui bisnisnya dengan memanfaatkan peluang ketersediaan inovasi teknologi serta dampaknya bagi kelangsungan dan pertumbuhan bisnis. Demikian juga dengan risiko yang dihadapinya yaitu suatu kejadian potensial, baik yang dapat diperkirakan (*anticipated*) maupun yang tidak dapat diperkirakan (*unanticipated*) yang berdampak negatif bagi nama baik Bank Rakyat Indonesia secara umum dan Bank BRI Unit ITN II Malang.

Beberapa contoh kasus *social engineering* yang terjadi di Bank BRI UnitITN II Malang:

1. Nasabah akan mendapat *Whatsapp,* SMS, telepon, link dengan memberikan informasi bahwa ada perubahan tarif transfer antar bank dari Rp6.500 tiap transaksi menjadi Rp150.000 per bulan. Penipu akan mengaku bahwa ia dari pihak Bank BRI dengan meyakinkan nasabah dengan profile menyerupai milik Bank BRI namun palsu. Penipu akan membimbing nasabah untuk mengikuti arahannya dan meminta data-data pribadi nasabah seperti nomor kartu ATM, kode CVV, kadaluarsa kartu ATM, PIN, *password*, *username*, kode OTP,dan M-token. Apabila nasabah mengikuti arahnnya, otomatis saldo yang ada direkening nasabah akan digunakan oleh penipu. Umunya transaksi yang dilakukan oleh penipu adalah sebuah pembayaran *e-wallet* atau aplikasi online *shop*.
2. Penipu akan menawarkan nasabah menjadi nasabah prioritas dengan penawaran hadiah

menarik lalu meminta data-data pribadi nasabah yang bersifat rahasia.

3. Tawaran layanan konsumen palsu kepada nasabah melalui media sosial seperti instagram, facebook, twitter, whatsapp, dan sebagainya. Melalui akun media sosial korban, penipu akan mengiirmkan sebuah link dengan mengatasnamakan Bank BRI untuk menawarkan bantuan secara online dan mengarahkan nasabah agar login di website palsu dengan menginput username serta password.
4. Tawaran menjadi agen laku pandai dengan meminta nasabah untuk menyebutkan data pribadi dan meminta nasabah untuk mentransfer uang guna untuk mendapatkan mesin EDC.
5. Penipu juga akan mengirimkan aplikasi bodong seperti file APK dan apabila nasabah mengklik file tersebut akan secara otomatis data nasabah akan terbaca oleh sistem dari penipu.

**Pencegahan dan Penyelesaian Tindak *Social Engineering* yang DilakukanBank BRI Unit ITN II Malang**

*Social engineering* berfokus pada mata rantai terlemah dalam rantai kemanan suatu perusahaan mulai dari teknologi informasi sampai manusia, nyatanya hampir semua teknologi informasi sangat bergantung pada manusia. Kelemahan ini bersifat umum dan terbebas dari hardware, software, platform, jaringan, dan usia peralatan. *Social engineering* telah mencapai tingkatan tertinggi kematangan sebagai strategi dalam membobol keamanan informasi. Keamanan ini digunakan perusahaan untuk melindungi apa yang dianggap aset-aset penting perusahaan. Keamanan yang terbaik pun dapat ditembus dengan *social engineering*, untuk mengurangi risiko tersebut, bank perlu untuk memberikan pelatihan dan edukasi kepada staf mereka mengenai ancaman keamanan dan

bagaimana caranya mengenali serangan.

Edukasi harus dilakukan dengan jelas dan mudah dipahami dan sebisa mungkin harus detail sehingga pengguna bisa memahami kerentanan atau kemungkinan resiko yang akan terjadi. Pihak bank bisa memberi informasi tentang jenis-jenis kerentanan yang ada semisal contoh kasus, selain itu akan lebih baik lagi kalau bank juga meyertakan tips agar terhindar dari potensi kejahatan fraud dalam edukasinya. Selain menambah pengetahuan, cara-cara ini juga diyakini bisa membuat nasabah lebih percaya diri dalam melakukan transaksi, dansemakin loyal dengan bank tempatnya menyimpan dana.

Cara pencegahan dan penyelesaian kasus *social engineering* yang dilakukan oleh pihak Bank BRI Unit ITN II Malang adalah sebagai berikut :

1. Memberikan kesadaran kepada nasaba tentang pentingnya sebuah informasi yang bersifat rahasia aeperti *password*, *username*, *m-token*, PIN, OTP, kode CVV, nomor kartu ATM, dan kadaluarsa ATM.
2. Memberitahu kepada nasabah modus-modus *social engineering* di media sosial.
3. Menginformasikan kepada nasabah mengenai akun sosial media Bank BRI yang asli sudah terverifikasi dan centang biru.
4. Memasang pengumuman/peringatan di *banking hall* supaya nasabah lebih berhati hati terhadap ancaman *social engineering.*
5. Berkoordinasi dengan petugas keamanan di lokasi ATM, jika ada perilaku mencurigakan dari terduga pelaku *social engineering* akan cepat diantisipasi.
6. Membuat iklan layanan masyarakat sosial medial tentang potensi bahaya *social engineering*.
7. Menayangkan video tentang bahaya *social engineering* di *banking hall* atau ruang tunggu nasabah.

8. Apabila nasabah sudah terlanjur mengikuti perintah penipu maka segera laporkan kepada *call center* Bank BRI dan segera melakukan perubahan PIN, *username*, dan *password.*
9. Jika mendapat pesan, link, telepon dari nomor yang tidak dikenal dan mengaku sebagai pegawai bank diabaikan saja, melakukan pemblokiran dan *report* nomor tersebut.

**Kendala Dalam Melakukan Pencegahan dan Penyelesaian Kasus *Social Engineering* yang Dilakukan Oleh Bank BRI Unit ITN II Malang**

Dalam menggunakan media sosial, masyarakat memiliki sifat untuk tetap eksis dengan melakukan *upload* kegiatan dalam bentuk foto, video, maupun tulisan. Perilaku ini seringkali berisikan informasi hal pribadi mereka sehingga dapat menyebabkan pengguna berada dalam posisi yang berbahaya dan berpotensi hilangnya privasi. Beberapa kasus seputar penyalahgunaan informasi kerap kali terjadi, banyak dari kasus tersebut dilakukan dengan tujuan untuk mendapatkan keuntungan bagi penipu. Penipu mengambil foto dan informasi nomor seluler korban melalui sosial media dan mengeditnya. Kasus mengenai penyalahgunaan informasi tersebut disebabkan oleh kurangnya kesadaran akan pentingnya menjaga privasi informasi di media sosial.

Ada beberapa kendala dalam pencegahan dan penyelesaian kasus *social engineering* yang terjadi di Bank BRI Unit ITN II seperti :

1. Nasabah kurang mengetahui apasaja modus-modus penipuan yang terjadi di dunia perbankan sehingga menyalahkan pihak Bank BRI karena mereka mengira bahwa itu memang benar-benar pihak BRI dan meminta saldo yang terkuras kembali lagi.

2. Saat pegawai Bank BRI memberikan edukasi mengenai informasi yang bersifat pribadi dan data-data yang bersifat rahasia harus disimpan sendiri dan jangan sampai bocor kepada orang lain termasuk pihak Bank BRI, nasabah tidak terlalu memerhatikan penjelasan yang telah diberikan.
3. Nasabah tergiur dan percaya atas penawaran yang dijanjikan oleh penipu sehingga langsung mengikuti arahannya.

Tidak banyak yang bisa mengetahui proses serangan rekayasa sosial terjadi. Maka dari itu diperlukan perlindungan yang dibentuk dari diri sendiri untuk mengatasi "mata rantai terlemah" pada sistem keamanan yaitu manusia (M. Jensen, 2020). Perlindungan ini dinamakan *human firewall*. Sama halnya seperti *firewall* yang melindungi jaringan komputer, *human firewall* adalah sebuah bentuk perlindungan yang sengaja dibentuk untuk mencegah berbagai serangan dari *hacker*, terutama serangan yang menggunakan teknik *social engineering*. Sebagaimana dijelaskan pada paragraf sebelumnya bahwa manusia adalah bagian yang rentan pada sistem keamanan. Pernyataan tersebut sangatlah jelas mengingat bahwa manusia adalah makhluk sosial yang tentu akan berfikir sebelum melakukan tindakan.

**Efektivitas Sistem Pencegahan dan Penyelesaian Kasus *Social Engineering* yang Dilakukan Oleh Bank BRI Unit ITN II Malang**

Pembukaan Undang-Undang Dasar 1945 merupakan pokok atau kaedah yang fundamental, mempunyai kedudukan yang tepat dan melekat Perusahaan Negara Republik Indonesia. Hal ini karena setiap alinea yang terdapat dalam Pembukaan UUD tercantum tujuan dan prinsip dasar yang hendak dicapai oleh bangsa negara Indonesia.

Salah satu tujuan bangsa yang terkandung dalam pembukaan UUD adalah tujuan keamanan nasional, yaitu untuk melindungi segenap bangsa Indonesia, seluruh tumpah darah Indonesia (Subekti, 2015).

Seiring dengan perkembangan zaman dan teknologi, bentuk ancaman dalam menghadapi keamanan nasional akan berubah. Kini ancaman dapat pula terjadi di dunia virtual. Cyber crime atau kejahatan di dunia siber. Beberapa kasus cyber crime diantaranya adalah kejahatan yang dilakukan oleh kelompok teroris memelalui media internet. Beberapa situs yang dianggap radikal yang disebarkan melalui propaganda radikalisme melalui media internet terbukti mengganggu keamanan nasional (Siagian, 2016).

## KESIMPULAN DAN SARAN

Perkembangan teknologi informasi membuat industri perbankan mengubah strategi bisnisnya dengan menjadikan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Seperti halnya pelayanan melalui ATM, BRIMO dan *Internet Banking* yang merupakan bentuk dari pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi yang berbasis teknologi. Faktor kepercayaan dan efisiensi serta kualitas layanan menjadi alasan bagi industri perbankan untuk selalu memperbarui bisnisnya dengan memanfaatkan peluang ketersediaan inovasi teknologi serta dampaknya bagi kelangsungan dan pertumbuhan bisnis.

Kasus *social engineering* yang terjadi di Bank BRI Unit ITN II Malang Nasabah akan mendapat *Whatsapp*, SMS, telepon, link dengan memberikan informasi bahwa ada perubahan tarif transfer antar bank dari Rp6.500 tiap transaksi menjadi Rp150.000 per

bulan. Penipu akan mengaku bahwa ia dari pihak Bank BRI dengan meyakinkan nasabah dengan profile menyerupai milik Bank BRI namun palsu. Penipu akan membimbing nasabah untuk mengikuti arahannya dan meminta data-data pribadi nasabah seperti nomor kartu ATM, kode CVV, kadaluarsa kartu ATM, PIN, *password*, *username*, kode OTP,dan M-token. Apabila nasabah mengikuti arahnnya, otomatis saldo yang ada direkening nasabah akan digunakan oleh penipu. Umunya transaksi yang dilakukan oleh penipu adalah sebuah pembayaran *e-wallet* atau aplikasi online *shop*. Tidak hanya itu, pelaku akan memberikan modus lainnya seperti tawaran menjadi nasabah prioritas, tawaran layanan konsumen palsu, tawaran menjadi agen laku pandai, dan juga mengirim file APK bodong.

Pencegahan dan penyelesaian kasus *social engineering* yang dilakukan oleh pihak Bank BRI Unit ITN II Malang dengan memberikan kesadaran kepada nasaba tentang pentingnya sebuah informasi yang bersifat rahasia aeperti *password, username, m-token*, PIN, OTP, kode CVV, nomor kartu ATM, dan kadaluarsa ATM. Tidak hanya itu, Bank BRI juga menyediakan iklan dan poster yang setiap hari diupdate melalui aplikasi BRIMO ynag berisi tentang modus- modus penipuan serta menginformasikan kontak sosial media Bank BRI yang asli telah terferivikasi dan centang biru.

Namun ada beberapa kendala yang terjadi di Bank BRI Unit ITN II Malang selama menangani kasus *social engineering* yaitu kurangnya kesadaran masyarakat tentang pentingnya keamanan informasi dan memahami tanggung jawab mereka, serta mengetahui tindakan untuk mengkontrol keamanan informasi yang cukup untuk melindungi data dan jaringan dalam organisasi. Tujuan dari meningkatkan kesadaran akan keamanan guna menyadarkan masyarakat, baik secara individual maupun dalam

organisasi akan risiko yang mereka hadapi dan merangsang mereka untuk mencegah risiko tersebut agar tidak terjadi.

Efektivitas sistem yang diberikan Bank Rakyat Indonesia (Persero) Tbk. dalam mencegah tindak *social engineering* mengurangi risiko nasabah tertipu oleh pelaku kejahatan. *Network security* menitikberatkan pada pengamanan peralatan jaringan data perusahaan dan isinya untuk menjaga keamanan informasi dari perusahaan tersebut maupun nasabahnya dengan melakukan perbaruan pada beberapa aplikasi yang digunakan nasabah dalam melakukan transaksinya sehari- hari.

*Social engineering* merupakan suatu kejahatan di bidang teknologi sehingga seluruh dunia menggunakan prinsip serba komputerisasi dan disitulah celah kejahatan yang bisa muncul kapan saja. Untuk mencegah bahkan melakukan penanganan apabila *social engineering* terus terjadi, bank dan pemerintah harus melakukan penegakan hukum melalui aparat negara seperti kepolisian, kejaksaan, bahkan badan intelejen pada institusi pemerintah baik itu Badan Intelejen Negara (BIN) maupun yang ada pada TNI-POLRI serta berkolaborasi dengan Kementerian Komunikasi dan Informasi untuk membatasi dan memantau perkembangan teknologi dengan menutup akses-akses yang dicurigai dapat menimbulkan suatu tindak pidana. Tentunya pekerjaan ini tidaklah mudah sehingga membutuhkan tenaga ahli yang mampu bertanggungjawab memantau bahkan melakukan penegakan hukum pada kasus *social engineering* yang telah diberikan pelatihan khusus serta menyiapkan komponen-komponen canggih untuk memantau *network and netsocial*. Tindak kejahatan *social engineering* disektor jasa keuangan dan perbankan semakin sering terjadi dan sangat merugikan nasabah juga nama baik bank menjadi tercemar, oleh karenanya para pelaku kejahatan *social engineering* harus mendapat hukuman yang berat

agar mereka menjadi jera untuk melakukannya lagi.

## DAFTAR PUSTAKA


Bungin, B. (2005). Dalam *Metodologi Penelitian Kuantitatif* (hal. 48, 122).

Bandung: Prenata Media Grup.

Indonesia, C. (2022, Maret 15). *Transaksi Digital BRI Tumbuh 96,7%*. Dipetik februari 20, 2023, dari CNBC INDONESIA: https://www.cnbcindonesia.com/tech/20220315161542-37-323005/wow-transaksi-digital-bri-tumbuh-967-ini-rinciannya

M. Jensen, R. W. (2020). Building the Human Firewall: Combating Phishing through Collective Action of Individuals Using Leaderboards. *SSRN Electron*.

Moloeng, L. J. (2000). Dalam *Metodologi Penelitian Kualitatif* (hal. 3, 135). Bandung: PT Remaja Rosdakarya.

Muhammad. (2008). Dalam *Metodologi Penelitian Islam Pendekatan Kualitatif*

(hal. 152). Jakarta: PT. Raja Grafindo Persada.

Nugraha, A. M. (2022). *Pangguna Aplikasi BRImo.* Jakarta: CNBC Indonesia. Rafizan, O. (2019). Analisis Penyerangan Social Engineering. *Peneliti Bidang Teknologi Informatika di Puslitbang Aptika & IKP Balitbang SDMKominfo*, 116-117.

Siagian. (2016). Dalam *Analisis Wacana Radikalisme pada Situs Online di Indonesia dalam Perspektif Keamanan Nasional.* Bogor: Studi Peperangan Asimetris Universitas Pertahanan.

Subekti. (2015). Dalam *Dinamika Konsolidasi Demokrasi: Dari Ide Pembaharuan Sistem Politik hingga ke Praktik Pemerintahan Demokratis.* Jakarta: Yayasan Pustaka Obor Indonesia.