https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE

Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

STRATEGI KOMUNIKASI KRISIS *PUBLIC RELATIONS* DALAM MENGHADAPI ANCAMAN *SOCIAL ENGINEERING (PHISHING)* DI ERA DIGITAL PADA PT BANK SYARIAH INDONESIA TBK

Ayu Amanda Viana[1], Eraskaita Ginting[2], Chairunnisah Putri Ayu Ningsih[3]

[1,2,3] Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Islam Negeri Raden Fatah
Jl. Prof. K. H. Zainal Abidin Fikri, Kota Palembang
e-mail: 2120701054@radenfatah.ac.id

ABSTRAK

Perkembangan teknologi informasi dan komunikasi mendorong transformasi besar pada sektor perbankan, termasuk PT Bank Syariah Indonesia Tbk (BSI). Digitalisasi memudahkan layanan, namun memunculkan risiko kejahatan siber seperti phishing dan social engineering yang merugikan finansial dan mengancam reputasi. Penelitian ini menganalisis strategi krisis Public Relations (PR) BSI dalam menghadapi phishing yang mengatasnamakan bank melalui platform digital. Metode yang digunakan adalah kualitatif deskriptif, dengan data dari wawancara Corporate Secretary, dokumentasi internal, publikasi Otoritas Jasa Keuangan (OJK), dan pemberitaan media. Analisis menggunakan Situational Crisis Communication Theory (SCCT) untuk melihat pemilihan strategi komunikasi sesuai atribusi tanggung jawab publik. Hasil penelitian menunjukkan empat strategi utama: (1) penyangkalan dengan menegaskan serangan berasal dari pihak eksternal; (2) edukasi dan literasi digital untuk meningkatkan kewaspadaan nasabah; (3) kolaborasi dengan OJK, Kominfo, media, dan Indonesia Anti Scam Center (IASC) untuk penanganan kasus; (4) pemulihan reputasi melalui komunikasi transparan, konsisten, dan sesuai prinsip syariah. Temuan menegaskan bahwa keberhasilan PR di era digital tidak hanya bergantung pada kecepatan respons, tetapi juga edukasi publik dan koordinasi lintas pihak untuk memulihkan kepercayaan dan memperkuat citra bank syariah.

Keywords: *Strategi, Public Relations, Phishing.*

1. PENDAHULUAN

Perkembangan dalam bidang teknologi telekomunikasi dan informatika didorong oleh persaingan yang ketat, sehingga mendorong lahirnya berbagai inovasi dan kemajuan dalam teknologi telematika. Hal ini tentunya berdampak signifikan terhadap pola dan strategi bisnis, termasuk di sektor perbankan. Keberagaman layanan, kemudahan, kecepatan, dan biaya jasa yang rendah menjadi harapan utama bagi nasabah. Kemajuan sistem perbankan sangat bergantung pada teknologi informasi. Semakin kompleks dan canggih fasilitas yang diterapkan oleh bank untuk mempermudah pelayanan, semakin sejalan pula dengan tingkat adopsi teknologi yang digunakan, baik untuk menunjang operasional internal maupun meningkatkan kualitas layanan bagi nasabah (Junaedi, 2017).

Berdasarkan data Bank Indonesia, pada triwulan III tahun 2024, transaksi perbankan digital mencapai 5.666,28 juta transaksi, meningkat 34,43% secara

https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

tahunan (YoY). Sebaliknya, transaksi pembayaran menggunakan kartu ATM/debit mengalami penurunan sebesar 8,59% (YoY) menjadi 1.738,53 juta transaksi. Peningkatan transaksi digital ini mencerminkan tingginya minat masyarakat untuk memanfaatkan kemudahan layanan perbankan modern. Fasilitas digital yang ditawarkan, *seperti internet banking*, *mobile banking*, dan pembayaran nontunai, memungkinkan nasabah melakukan transaksi kapan saja dan di mana saja, sehingga tidak hanya mempercepat proses keuangan tetapi juga mengurangi kebutuhan akan kunjungan fisik ke bank (Rismasari, 2025).

Dampak positif dari perkembangan teknologi tidak hanya dirasakan secara konstruktif, tetapi juga dimanfaatkan oleh pihak-pihak yang memiliki niat buruk untuk mencari keuntungan melalui tindakan kriminal. Seperti dijelaskan dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, teknologi informasi bersifat pedang bermata dua, karena selain berperan dalam meningkatkan kesejahteraan, pertumbuhan, dan peradaban masyarakat, teknologi juga dapat digunakan sebagai sarana yang efisien untuk melakukan tindakan melawan hukum (Ekayani, 2023).

Pelaku tindak kejahatan dapat beraksi di mana saja dan dengan cara apa pun selama terdapat celah untuk melakukan aksinya. Dalam ranah internet, peluang terjadinya tindak kejahatan sangat tinggi dan penegakan hukumnya pun sulit dilakukan karena mayoritas identitas pengguna bersifat anonim atau fiktif. Fenomena inilah yang kemudian dikenal dengan istilah *Cyber Crime* atau kejahatan dunia maya (Puspitasari, 2018).

Gibbs (2020) menyatakan bahwa meningkatnya kerentanan terhadap *cyber crime* terkait erat dengan cepatnya perkembangan teknologi. Perkembangan teknologi tidak hanya membawa kemudahan, tetapi juga membuka peluang baru bagi munculnya tindak penipuan (*fraud*), terutama di sektor perbankan, yang semakin beragam seiring kemajuan teknologi. Setiap kemudahan dan keuntungan yang diberikan teknologi juga menghadirkan potensi kerugian dan kelemahan. Salah satu dampak negatifnya adalah munculnya berbagai bentuk kejahatan dalam dunia digital, seperti pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (ITE), termasuk *phishing*, *hacking*, *carding*, *skimming*, dan praktik kejahatan siber lainnya (Putri, 2022).

Menurut data APJII, penipuan online tercatat sebagai kasus tertinggi dalam kejahatan siber dengan persentase 32,5%. Angka ini melonjak signifikan sebesar 22,2% dibandingkan tahun 2023 yang hanya 10,3%. Ketua Umum APJII, Muhammad Arif, pada akhir Januari menyampaikan bahwa berbagai bentuk kejahatan siber, seperti pencurian data pribadi dan penipuan online, masih menjadi persoalan serius dengan tren peningkatan yang mengkhawatirkan.

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

Peningkatan signifikan kasus penipuan online ini menunjukkan bahwa selain serangan berbasis teknologi, pelaku kejahatan siber juga semakin memanfaatkan faktor manusia sebagai celah keamanan. Salah satu metode yang sering digunakan adalah *social engineering* atau *human hacking*, di mana pelaku memanipulasi psikologis korban untuk memperoleh informasi rahasia (Prastya, 2024).

Social engineering atau *human hacking* merupakan teknik serangan yang memanfaatkan kelemahan psikologis manusia untuk mendapatkan akses terhadap data atau informasi yang bersifat rahasia. Berbeda dengan metode peretasan berbasis teknologi, *social engineering* lebih menitikberatkan pada manipulasi psikologis korban agar secara sukarela memberikan informasi yang diminta pelaku. Kondisi ini menjadikan manusia sebagai mata rantai terlemah dalam sistem keamanan informasi, sebab faktor psikologis cenderung dinamis, mudah dipengaruhi, dan rentan dimanfaatkan oleh pihak yang tidak bertanggung jawab. CNN Indonesia mencatat bahwa setiap bulan sekitar 2.000 nasabah bank swasta di Indonesia menjadi korban kejahatan siber dengan modus *social engineering* (Anindya, 2023).

Data tersebut memperlihatkan bahwa *social engineering* membawa dampak yang cukup besar bagi sektor perbankan, terutama dalam upaya melindungi kerahasiaan data nasabah serta menjaga kepercayaan masyarakat terhadap lembaga keuangan. Sasaran utama dari praktik ini umumnya adalah nasabah bank, pengguna layanan dompet digital, konsumen *e-commerce*, hingga individu yang aktif berinteraksi melalui media sosial. Hal ini menunjukkan bahwa semakin tinggi tingkat ketergantungan masyarakat pada layanan digital, semakin besar pula peluang pelaku kejahatan memanfaatkan celah untuk melakukan penipuan.

Pendekatan sosio-teknik dalam *social engineering* mencakup berbagai metode yang memanfaatkan kelemahan manusia dan sistem digital untuk memperoleh informasi sensitif. Salah satu bentuk yang paling umum adalah *phishing*, di mana penyerang berupaya mengekstraksi data pribadi melalui media digital, seperti email palsu yang tampak berasal dari sumber resmi atau situs web tiruan. Serangan *phishing* sering dirancang untuk memanipulasi psikologis korban, dengan menargetkan banyak orang sekaligus. Situs jejaring sosial juga kerap digunakan untuk menambang informasi calon korban, sehingga pesan yang dikirim tampak personal dan dipercayai berasal dari teman dekat (Safitri, 2020).

Anti-*Phishing Working Group* (APWG) menjelaskan bahwa *phishing* merupakan bentuk kejahatan siber yang memanfaatkan kombinasi teknik rekayasa sosial dan kemajuan teknologi untuk memperoleh keuntungan bagi pelaku. Dalam praktiknya, keberhasilan serangan *phishing* sangat bergantung pada kemampuan penipu untuk memanipulasi perilaku dan psikologi korban, sehingga korban secara tidak sadar memberikan

https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

informasi sensitif, seperti kata sandi, nomor rekening, atau data pribadi lainnya. *Phishing* bukan hanya sekadar serangan berbasis teknologi, tetapi juga memerlukan strategi psikologis yang cermat agar korban percaya terhadap pesan atau situs palsu yang dibuat menyerupai sumber resmi. Dengan demikian, *phishing* menjadi salah satu ancaman utama bagi keamanan digital, terutama di sektor perbankan dan layanan keuangan, di mana informasi pribadi dan transaksi finansial menjadi target yang sangat bernilai (Ilyas, 2023).

Dalam konteks perbankan, serangan *phishing* dapat merugikan nasabah dan lembaga keuangan secara signifikan. Contohnya, pada Januari 2023, Direktorat Tindak Pidana Siber Bareskrim Polri mengungkap kasus penipuan yang melibatkan 13 tersangka dan merugikan 493 nasabah bank dengan total kerugian mencapai Rp12 miliar. Modus operandi yang digunakan adalah modifikasi aplikasi (APK) dan pengiriman tautan *phishing* melalui pesan *WhatsApp* yang tampak resmi, seperti notifikasi pengiriman paket atau promo perbankan (Yuspin, 2024).

Di Indonesia, sektor perbankan terdiri dari berbagai jenis lembaga, salah satunya adalah PT Bank Syariah Indonesia (BSI). Sebagai salah satu institusi terkemuka dalam industri perbankan syariah nasional, BSI juga menghadapi berbagai potensi ancaman dan risiko yang terkait dengan keamanan informasi dan serangan siber. Dalam perannya sebagai bagian penting dari ekosistem keuangan, BSI dituntut untuk mengelola tantangan yang kompleks dalam menjaga kerahasiaan data nasabah serta mempertahankan tingkat kepercayaan masyarakat. Meningkatnya frekuensi serangan siber, termasuk *phishing*, *malware*, dan gangguan layanan digital, menekankan urgensi bagi BSI untuk menerapkan langkah-langkah keamanan yang efektif, meningkatkan kesadaran digital nasabah, serta memperkuat sistem perlindungan data agar tetap mampu menghadapi risiko keamanan yang terus berkembang (Dianita, 2021).

Dalam situasi seperti ini, peran *Public Relations* (PR) menjadi sangat penting, terutama dalam menjaga kepercayaan publik dan meminimalisir dampak reputasi akibat serangan *phishing*. *Public Relations* bertanggung jawab untuk membangun komunikasi yang jelas, cepat, dan transparan kepada nasabah maupun masyarakat luas agar tidak menimbulkan kepanikan serta misinformasi. Melalui strategi komunikasi krisis, *Public Relations* harus mampu menyampaikan klarifikasi resmi, memberikan edukasi terkait modus *social engineering*, serta menegaskan langkah-langkah preventif yang telah dilakukan oleh pihak bank (Ardiani, 2022).

Selain itu, *Public Relations* juga berfungsi sebagai mediator antara perusahaan dan publik, dengan memastikan pesan yang disampaikan konsisten baik di media massa maupun saluran komunikasi digital resmi seperti *website*, media sosial, dan aplikasi

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

perbankan. Pendekatan ini tidak hanya bertujuan mengendalikan isu, tetapi juga menjadi sarana edukasi publik mengenai pentingnya kewaspadaan terhadap *phishing*. Dengan demikian, *Public Relations* berperan sentral dalam menjaga citra dan reputasi PT Bank Syariah Indonesia agar tetap dipercaya sebagai lembaga keuangan syariah yang aman dan profesional di tengah tantangan era digital (Fitria, 2021).

Berdasarkan latar belakang tersebut, peneliti memilih topik ini karena maraknya kasus *phishing* yang mengatasnamakan Bank, meskipun bukan dilakukan oleh pihak bank, tetap menimbulkan ancaman serius terhadap citra, reputasi, dan kepercayaan publik. Hal ini menuntut adanya manajemen komunikasi krisis *Public Relations* yang tepat, agar masyarakat tidak terjebak dalam misinformasi dan tetap percaya terhadap keamanan layanan digital BSI. Oleh karena itu, penelitian ini berfokus pada komunikasi krisis *Public Relations* dalam menghadapi ancaman *social engineering (phishing*) di era digital pada PT Bank Syariah Indonesia Tbk.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan fokus pada analisis deskriptif terhadap strategi manajemen komunikasi krisis *Public Relations* dalam menghadapi ancaman *social engineering (phishing)* di era digital pada PT Bank Syariah Indonesia Tbk. Kerangka analisis penelitian mengacu pada *Situational Crisis Communication Theory (SCCT)* yang pertama kali dikemukakan oleh Timothy W. Coombs dan Sherry J. Holladay pada tahun 1995, kemudian diperluas dan diperkuat kembali oleh Coombs pada tahun 2007 melalui publikasi yang lebih komprehensif. Teori ini memberikan landasan konseptual mengenai bagaimana organisasi dapat memilih strategi komunikasi krisis yang tepat, bergantung pada tingkat atribusi tanggung jawab yang diberikan publik terhadap suatu krisis (Virginia et al., 2025).

Teknik pengumpulan data dalam penelitian ini dilakukan melalui wawancara mendalam dengan pihak *Public Relations/Corporate Secretary* dan staf yang terlibat dalam penanganan komunikasi krisis, serta melalui dokumentasi berupa laporan resmi perusahaan, publikasi Otoritas Jasa Keuangan (OJK), dan pemberitaan media yang relevan terkait kasus *phishing.*

Subjek penelitian adalah *Public Relations* PT Bank Syariah Indonesia Tbk, sedangkan objek penelitian adalah manajemen komunikasi krisis dalam menangani ancaman *social engineering (phishing)*. Sumber data yang digunakan meliputi data primer, yaitu hasil wawancara dengan informan kunci dari pihak bank, serta data sekunder berupa dokumen resmi, buku, jurnal, dan referensi lainnya yang mendukung penelitian ini.

3. HASIL DAN PEMBAHASAN

A. Kronologi Kasus *Phishing* yang Mengatasnamakan BSI

Kasus penipuan yang mengatasnamakan PT Bank Syariah Indonesia (BSI) menjadi contoh nyata

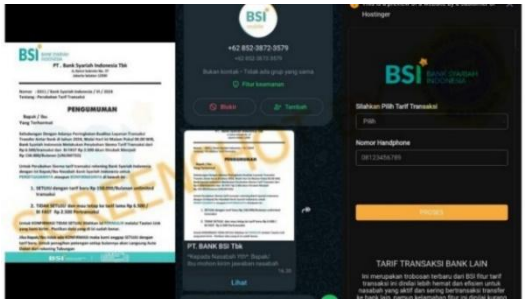
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE

Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

bagaimana kejahatan *social engineering* dapat merugikan nasabah sekaligus menimbulkan tantangan reputasi bagi lembaga perbankan. Salah satu kejadian menonjol terjadi pada tanggal 24 Juni 2024, seorang nasabah BSI berinisial HA di Malang, Jawa Timur, menerima pesan melalui *WhatsApp* yang menginformasikan perubahan tarif transaksi dan disertai tautan yang menyerupai portal resmi bank. Tautan ini dirancang sedemikian rupa sehingga secara visual hampir identik dengan laman resmi BSI, sehingga memberikan kesan resmi dan meyakinkan (Lensa IDN, 2024).

Kejadian ini menunjukkan bagaimana penipu menggunakan teknik *social engineering*, yaitu manipulasi psikologis untuk memanfaatkan kepercayaan korban terhadap institusi perbankan. Dalam pesan tersebut, berisi informasi adanya perubahan tarif administrasi bulanan, dari Rp 8.000 menjadi Rp 150.000. Pesan tersebut menyertakan tautan menuju situs palsu yang dibuat sedemikian rupa untuk menipu korban agar menyerahkan informasi pribadi, seperti *User ID*, *PIN*, dan nomor rekening. Selain itu, pelaku memberikan tekanan dengan menetapkan batas waktu 24 jam untuk pengiriman data, disertai ancaman bahwa jika tidak memenuhi permintaan, kenaikan tarif tersebut akan dianggap otomatis disetujui oleh nasabah (Ekayani, 2023).



Gambar 1. Pesan yang diterima
(Sumber: TurnBackHoax.id, 2024)

Isi pesan yang diterima oleh korban mengatasnamakan Bank Syariah Indonesia (BSI) dengan bahasa yang seolah resmi dan mendesak, yaitu:

"Kepada Yth. Nasabah BSI, Bapak/Ibu dimohon untuk segera memberikan tanggapan atas informasi yang telah kami sampaikan di atas agar tidak diberlakukan tarif baru secara otomatis oleh sistem. Untuk menentukan pilihan SETUJU atau TIDAK SETUJU, silakan konfirmasi melalui tautan formulir di bawah ini" (TurnBackHoax.id, 2024).

Pesan ini dirancang untuk membangkitkan rasa urgensi dan memanfaatkan kepatuhan nasabah terhadap instruksi yang tampak resmi. Setelah korban menerima pesan, pelaku melakukan panggilan telepon dengan berpura-pura sebagai staf resmi bank. Selama percakapan tersebut, korban diberi arahan agar melakukan transaksi melalui aplikasi pihak ketiga, dengan nada yang terdengar mendesak dan persuasif. Strategi ini merupakan bagian dari teknik social engineering yang memanfaatkan tekanan psikologis, di mana korban dipaksa mengambil keputusan cepat tanpa memverifikasi informasi.

Tekanan yang diberikan oleh pelaku

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
sinta S5
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

membuat korban mengikuti semua instruksi yang diberikan, meskipun secara logis tindakan tersebut tampak berisiko. Modus seperti ini menekankan pentingnya pemahaman publik terkait tanda-tanda komunikasi palsu, serta perlunya edukasi berkelanjutan untuk membangun kesadaran terhadap penipuan digital. Selain itu, interaksi telepon ini menunjukkan bagaimana persepsi korban terhadap otoritas bank dapat dimanfaatkan oleh pihak eksternal. Public Relations memiliki peran penting untuk memastikan publik memahami bahwa komunikasi resmi hanya melalui saluran tertentu, sehingga setiap tindakan preventif dapat mengurangi dampak negatif terhadap reputasi bank (Langoday, 2025).

Kerugian finansial yang dialami oleh korban menunjukkan adanya kebutuhan mendesak bagi institusi perbankan untuk memiliki prosedur komunikasi krisis yang siap digunakan dalam menghadapi ancaman serupa. Dalam perspektif *Situational Crisis Communication Theory* (SCCT), kasus ini dapat dikategorikan sebagai krisis yang berasal dari pihak eksternal, di mana bank termasuk dalam *Victim Cluster* atau kelompok korban. Hal ini menekankan bahwa strategi komunikasi yang dipilih sebaiknya tidak menyalahkan pihak internal bank, melainkan fokus pada penyampaian informasi yang jelas, transparan, dan penuh empati. *Public Relations* berperan penting dalam menyeimbangkan respons yang cepat dan efektif sambil tetap menjaga reputasi institusi (Hardian et al., 2025).

B. Komunikasi Krisis *Public Relations* dalam Menghadapi Kasus *Phishing*

1. Strategi Denial (Penyangkalan Langsung)

Salah satu respons krisis yang dijalankan oleh *Public Relations* (PR) Bank Syariah Indonesia (BSI) ketika menghadapi maraknya kasus *phishing* di *WhatsApp* adalah penggunaan strategi denial atau penyangkalan langsung, di mana organisasi berupaya untuk menolak keterlibatan langsung terhadap isu atau krisis yang terjadi. BSI menegaskan bahwa berbagai pesan yang dikirimkan melalui *WhatsApp* tanpa tanda verifikasi centang hijau bukanlah berasal dari pihak resmi bank, melainkan ulah pihak tidak bertanggung jawab yang berusaha melakukan *social engineering* (Muadz, 2025).

> *"Kami menegaskan bahwa informasi tersebut tidak berasal dari Bank Syariah Indonesia. Layanan resmi WhatsApp Bank Syariah Indonesia hanya tersedia melalui nomor 0815-8411-4040 yang telah memiliki tanda centang biru (verified). Kami mengingatkan masyarakat untuk selalu waspada terhadap akun-akun palsu yang mengatasnamakan Bank Syariah Indonesia. Jangan menanggapi atau memberikan informasi pribadi kepada pihak yang tidak resmi"(Bank Syariah Indonesia, 2025).*

Penyangkalan ini memiliki dua tujuan utama. Pertama, menjaga agar publik tidak terjebak pada persepsi keliru bahwa pesan-pesan tersebut memang dikirimkan

https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

oleh BSI. Kedua, melindungi reputasi perusahaan agar tidak ikut terseret dalam pusaran krisis yang diciptakan oleh pihak eksternal. Penyangkalan langsung juga diikuti dengan pernyataan resmi dari manajemen BSI melalui media massa, laman resmi, serta unggahan di kanal media sosial bank, yang menekankan bahwa BSI tidak pernah meminta data pribadi, PIN, OTP, ataupun biaya administrasi melalui jalur komunikasi *WhatsApp*.

Dari sisi lain, langkah denial ini relevan karena BSI secara posisi berada dalam kategori *victim cluster*, yaitu perusahaan dianggap sebagai korban dari serangan pihak luar, bukan pelaku atau penyebab krisis. Oleh karena itu, strategi penyangkalan justru memperkuat posisi BSI sebagai institusi yang ikut dirugikan oleh keberadaan modus penipuan digital. Namun, penyangkalan tidak hanya berhenti pada deklarasi semata. *Public Relations* BSI melengkapinya dengan bukti-bukti konkret, seperti mempublikasikan nomor resmi *WhatsApp* BSI yang sudah memiliki verifikasi centang hijau (0815-8411-4040), serta menampilkan imbauan visual yang konsisten untuk memperjelas identitas kanal resmi komunikasi perusahaan.

Penyampaian denial ini dipilih dengan gaya komunikasi yang sederhana, lugas, dan mudah dipahami oleh seluruh lapisan nasabah, baik melalui siaran pers, unggahan di Instagram, maupun notifikasi di aplikasi mobile banking BSI Mobile. Strategi ini menegaskan bahwa perusahaan berusaha tampil proaktif dalam menjawab isu, sehingga publik dapat segera membedakan antara saluran komunikasi resmi dengan saluran palsu yang digunakan pelaku *phishing*.

Dengan demikian, strategi denial dalam kasus ini tidak sekadar bentuk pembelaan diri, melainkan sebuah instrumen *Public Relations* untuk meredam keresahan publik, memperjelas sumber krisis, serta mengembalikan kendali komunikasi ke tangan institusi resmi. Denial menjadi pintu masuk utama dalam keseluruhan strategi krisis, sebelum dilanjutkan pada strategi yang lebih konstruktif seperti edukasi dan literasi digital.

2. Edukasi dan Literasi Digital

Setelah menegaskan penyangkalan, BSI memperkuat langkah penanganan krisis dengan mengedepankan strategi edukasi publik. Hal ini dilakukan karena krisis *phishing* di era digital pada dasarnya memanfaatkan kerentanan literasi digital masyarakat. Banyak nasabah belum memahami bahwa pesan *WhatsApp* dengan format tertentu dapat menjadi sarana pencurian data. Oleh sebab itu, *Public Relations* BSI mengambil peran sebagai komunikator edukatif yang memberikan pencerahan bagi masyarakat luas.

Strategi edukasi dijalankan melalui berbagai kanal komunikasi, mulai dari unggahan infografis di media sosial, artikel edukatif di laman resmi perusahaan, hingga penyuluhan digital *security awareness* dalam program tanggung jawab sosial BSI. Infografis misalnya dibuat dengan bahasa yang sederhana, penuh visualisasi, serta langsung membandingkan perbedaan antara

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

pesan palsu dan pesan resmi. Edukasi semacam ini menjadi penting, karena menurut data Otoritas Jasa Keuangan (OJK), tren pengaduan terkait penipuan digital meningkat signifikan pada 2023–2024, dengan salah satu modus tertinggi berupa *phishing* melalui *WhatsApp* (Putri, 2024).

Pernyataan ini menegaskan bahwa strategi penyangkalan tidak hanya sebatas membantah keterlibatan, tetapi juga dilengkapi dengan langkah pencegahan berupa edukasi kepada masyarakat guna menjaga kepercayaan nasabah dan mempertahankan citra positif bank. Selain itu, BSI menyelipkan edukasi literasi digital langsung ke aplikasi *BSI Mobile*. Melalui notifikasi *pop-up*, nasabah diberitahu bahwa BSI tidak pernah meminta kode OTP atau password untuk alasan apapun (Sari, 2025).

Gambar 2. Edukasi Digital
(Sumber: Bank BSI, 2025)

Gambar 3. Edukasi Digital
(Sumber: Bank BSI, 2025)

Strategi ini sangat efektif, karena pesan edukasi hadir pada momen penggunaan layanan, sehingga langsung relevan dengan perilaku pengguna. Dari perspektif *Public Relations*, strategi edukasi ini mencerminkan peran sebagai educator yang tidak hanya reaktif dalam menanggapi isu, tetapi juga preventif untuk mencegah terulangnya kasus serupa. Dengan meningkatkan literasi digital nasabah, *Public Relations* BSI membangun kapasitas publik agar mampu melindungi diri sendiri dari ancaman kejahatan siber (Rahayu, 2025).

Edukasi juga berfungsi memperluas tanggung jawab sosial perusahaan (*corporate social responsibility*/CSR) di ranah digital. Dengan mengedepankan literasi keamanan transaksi, BSI tidak hanya menjaga kepercayaan nasabah, tetapi juga berkontribusi pada agenda nasional peningkatan inklusi dan literasi keuangan digital yang dicanangkan oleh OJK dan Bank Indonesia. Pada akhirnya, keberhasilan edukasi digital ini tidak hanya diukur dari menurunnya jumlah korban *phishing*, tetapi juga dari meningkatnya kesadaran masyarakat untuk lebih kritis dan berhati-hati dalam menerima pesan digital (Bank Syariah Indonesia, 2025).

3. Kolaborasi dengan Pihak Eksternal

Krisis *phishing* tidak mungkin diselesaikan hanya dengan komunikasi internal perusahaan. Oleh karena itu, BSI juga menjalankan strategi kolaborasi dengan pihak eksternal sebagai bentuk sinergi penanganan krisis. Kolaborasi ini mencakup koordinasi dengan OJK, Bank Indonesia, Kementerian Komunikasi dan Informatika (Kominfo) Bank Syariah

https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

Indonesia, 2025).

Public Relations BSI berperan sebagai jembatan komunikasi antara institusi eksternal dengan publik. Misalnya, ketika OJK mengeluarkan peringatan resmi terkait maraknya penipuan digital, BSI mengamplifikasi pesan tersebut melalui kanal internal bank, sehingga lebih mudah diterima oleh nasabah. Kolaborasi dengan Kominfo dilakukan dalam bentuk pelaporan nomor telepon dan tautan *phishing* untuk kemudian diblokir Bank Syariah Indonesia, 2025).

Selain kolaborasi dengan regulator, BSI juga menjalin kerja sama dengan media massa arus utama. Media digunakan sebagai saluran komunikasi krisis untuk menyebarkan klarifikasi dan edukasi secara lebih luas. Dengan adanya liputan media, pesan denial dan edukasi dari BSI memperoleh legitimasi, karena publik lebih cenderung mempercayai informasi yang dikonfirmasi oleh pihak ketiga yang kredibel (Maulana, 2024).

Kolaborasi juga dilakukan dengan menindaklanjuti laporan nasabah dengan mengajukan pengaduan ke Indonesia Anti *Scam Center* (IASC), lembaga yang berperan sebagai pusat pelaporan dan koordinasi penanganan kejahatan siber. Setiap pengaduan disertai nomor laporan resmi, sehingga korban dan pihak terkait dapat memantau perkembangan penanganannya secara transparan. Selain itu, bank memberikan panduan kepada nasabah untuk melakukan pengecekan secara mandiri melalui situs resmi IASC di https://iasc.ojk.go.id dengan memilih menu "Cek Laporan" dan memasukkan nomor yang telah diberikan. Dalam salah satu kasus, bank menyampaikan:

> *"Berdasarkan laporan yang diterima, nasabah diduga mengalami penipuan berbasis social engineering. Karena adanya perpindahan dana ke bank lain, laporan telah kami teruskan ke IASC dengan nomor 4444444 (disamarkan). Nasabah dapat memantau status laporan melalui laman resmi IASC dengan memilih menu Cek Laporan dan memasukkan nomor pelaporan tersebut"(Bank Syariah Indonesia, 2025).*

Langkah ini menunjukkan kesigapan bank sekaligus memberikan edukasi kepada nasabah agar lebih memahami mekanisme pelaporan resmi dalam menghadapi tindak kejahatan digital.

4. Penguatan Reputasi dan Kepercayaan Publik

Langkah terakhir yang tidak kalah penting dalam komunikasi krisis *Public Relations* BSI adalah penguatan reputasi dan kepercayaan publik. Dalam krisis *phishing*, reputasi perusahaan berpotensi tergerus jika publik menganggap bank tidak mampu melindungi data dan transaksi nasabah. Oleh karena itu, BSI secara konsisten membangun narasi positif mengenai komitmen perusahaan terhadap keamanan digital.

Penguatan reputasi dilakukan melalui tiga pendekatan. Pertama, *consistency of message*. Semua kanal

https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

komunikasi BSI, baik media sosial, *website*, aplikasi, maupun *customer service*, menyampaikan pesan yang konsisten mengenai keamanan digital dan prosedur resmi komunikasi bank. Konsistensi ini membuat publik yakin bahwa BSI memiliki sistem komunikasi yang solid, bukan sekadar reaktif menghadapi isu (Rohmah, 2023).

Kedua, *transparency*. BSI tidak menutup-nutupi adanya potensi kerugian akibat *phishing*, tetapi justru menyampaikan secara terbuka mekanisme pengaduan, saluran resmi, serta langkah penanganan jika nasabah menjadi korban. Transparansi ini penting untuk menunjukkan bahwa perusahaan tidak bersikap defensif, melainkan solutif dalam menghadapi krisis (Indasari, 2025).

Ketiga, *value reinforcement*. BSI mengaitkan narasi penanganan krisis dengan nilai-nilai syariah yang dijunjung tinggi, seperti kejujuran *(shidq)*, amanah, dan kepedulian sosial. Dengan membingkai isu *phishing* sebagai ancaman terhadap prinsip keadilan dan keamanan dalam transaksi syariah, *Public Relations* BSI berhasil mengintegrasikan strategi krisis dengan identitas brand yang berlandaskan nilai Islam (Shipman, 2024).

Penguatan reputasi juga ditopang dengan penghargaan dan sertifikasi keamanan digital yang diperoleh BSI dari lembaga eksternal. *Public Relations* memanfaatkan capaian ini sebagai bukti objektif bahwa perusahaan terus berupaya memperkuat sistem keamanan informasi. Publikasi penghargaan tersebut diposisikan sebagai *symbolic reassurance*, yakni simbol yang menenangkan publik bahwa BSI tidak tinggal diam dalam menghadapi ancaman digital (Faucher, 2024).

Dari perspektif jangka panjang, kepercayaan publik terhadap BSI tidak hanya dipulihkan, tetapi juga berpotensi meningkat, karena perusahaan menunjukkan kemampuan adaptif dalam mengelola krisis. Reputasi yang kokoh menjadi aset penting, terutama dalam industri perbankan syariah yang sangat bergantung pada modal kepercayaan.

4. KESIMPULAN

Perkembangan teknologi informasi dan telekomunikasi telah mendorong transformasi besar di sektor perbankan, termasuk di Bank Syariah Indonesia (BSI). Digitalisasi layanan memberikan kemudahan dan efisiensi bagi nasabah, namun di sisi lain memunculkan risiko kejahatan siber, seperti *phishing* dan *social engineering*, yang memanfaatkan kelemahan manusia dan celah keamanan digital. Fenomena ini tidak hanya merugikan nasabah secara finansial, tetapi juga mengancam citra dan reputasi lembaga perbankan.

Dalam konteks tersebut, peran *Public Relations* (PR) menjadi krusial untuk memitigasi dampak krisis. Melalui pendekatan *Situational Crisis Communication Theory* (SCCT), BSI memposisikan diri sebagai pihak korban dan menerapkan strategi komunikasi yang tepat. Langkah-langkah yang dilakukan meliputi:

1. Strategi denial (penyangkalan) untuk menegaskan bahwa serangan berasal

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

dari pihak eksternal dan bukan dari bank.
2. Edukasi dan literasi digital untuk meningkatkan kesadaran nasabah agar lebih waspada terhadap modus penipuan.
3. Kolaborasi dengan pihak eksternal seperti OJK, Kominfo, media massa, dan Indonesia *Anti Scam Center* (IASC) untuk memperkuat respons dan mempermudah pelaporan kasus.
4. Penguatan reputasi dan kepercayaan publik melalui pesan yang konsisten, transparansi informasi, dan peneguhan nilai-nilai syariah sebagai identitas brand.

Keseluruhan strategi ini menunjukkan bahwa komunikasi krisis tidak hanya bertujuan meredam isu, tetapi juga bersifat preventif dan edukatif, sehingga dapat memulihkan serta meningkatkan kepercayaan publik. Penelitian ini menegaskan bahwa keberhasilan manajemen komunikasi krisis Public Relations di era digital sangat bergantung pada kecepatan respons, koordinasi lintas pihak, dan kemampuan memanfaatkan berbagai saluran komunikasi untuk menyampaikan pesan yang jelas, terpercaya, dan bernilai bagi pemangku kepentingan.

5. DAFTAR PUSTAKA

Aurelia, G., Ugahari, A., & Apriliani, R. (2025). Analisis Situational Crisis Communication Theory (SCCT) pada strategi komunikasi krisis brand Erspo dalam kasus kontroversi jersey Timnas Indonesia. *Mukasi*, 4(3), 1000–1012.

Ardiani, N. L., & Wibowo, B. (2022). Strategi public relations dalam mengelola krisis reputasi akibat serangan siber pada lembaga keuangan. *Jurnal Ilmu Komunikasi*, 14(2), 115–128.

Azhar, F. (2023). Analisis strategi komunikasi Bank Syariah Indonesia (BSI) dalam penanganan krisis serangan siber perbankan. Kementerian Keuangan Republik Indonesia.

Bairizki, A., Irwansyah, R., Arifudin, O., Asir, M., Wijiharta, W., Ganika, G., Karyanto, B., Lewaherilla, N.

Nasfi, Nugroho, L., Hasbi, I., & Marietza, F. (2021). *Manajemen Perubahan*. Bandung: Widina Bhakti Persada.

Dewi, A. R., Sya'bania, Z. N., Daffa, M. R., & Karina, N. (2025). Tantangan TV Muhammadiyah di era digital dalam menghadapi perubahan konsumsi digital. In *Konstelasi Media di Era Digital: Hierarki, Opini Publik, dan Dialektika Gender*.

Dianita, I., Irawan, H., & Mulya, A. D. S. (2021). Peran Bank Syariah Indonesia dalam pembangunan ekonomi nasional. *Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam*, 3(2).

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

Ekayani, L., Djanggih, H., & Suong, M. A. (2023). Perlindungan hukum nasabah terhadap kejahatan pencurian data pribadi (phising) di lingkungan perbankan. *Journal of Philosophy (JLP)*, 4(1).

Fitria, R., & Rahmawati, N. (2021). Manajemen komunikasi krisis perbankan di era digital: Studi pada respon bank terhadap kasus phishing. *Jurnal Komunikasi Massa*, 5(1), 45–58.

Ilyas, F. Q. (2023). *Formula model penanganan phishing pada Bank BRI: Analisis, dampak, dan implementasi* (Tesis, Program Magister Manajemen, Universitas Hasanuddin).

Indrayani, H. (2017). Etika advokasi public relations dalam manajemen krisis reputasi. *Interaksi: Jurnal Ilmu Komunikasi*, 5(1), 68–77.

Junaedi, D. I. (2017). Antisipasi dampak social engineering pada bisnis perbankan. *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*, 11(1).

Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering: Studi kasus data breach di Indonesia. *Prosiding Manajerial dan Kewirausahaan VIII*, 9–17.

Langoday, Y. R. (2025). *Representasi distopia digital dan hiperrealitas dalam prosa fiksi pada empat serial film "The Matrix"* (Tesis Magister Pendidikan). Universitas Negeri Makassar.

Maulana, N. (2024). Manajemen krisis PT. BSI Tbk pasca peretasan data. *J-Innovative*.

Muadz, A. M., Syarif, A., & Manggaga, I. P. (2025). Strategi komunikasi krisis Humas PLN dalam menangani pemadaman listrik di Sulawesi Selatan, Tenggara, dan Barat (Oktober 2023–Januari 2024): Pendekatan teori SCCT. *Jurnal Ilmu Komunikasi UHO: Jurnal Penelitian Kajian Ilmu Komunikasi dan Informasi*, 10(3).

Putri, R. N. S. (2022). Analisa pola–pola sosialisasi pencegahan modus social engineering oleh bank melalui media website dan media sosial Twitter (Tesis, Program Magister Akuntansi, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia).

Putri, R. N. S., & Hendi, H. Y. P. (2024). Analysis of social engineering prevention socialization patterns through websites and Twitter. *Journal of Contemporary Accounting*,

JURNAL ILMIAH ILMU KOMUNIKASI COMMUNIQUE
https: www.ejurnal.stikpmedan.ac.id
Vol. 8 No. 1, 13 Oktober 2025
e-ISSN LIPI: 2622-7290
Submit Date: 20 Agustus 2025 Accepted Date: 27 Agustus 2025 Published Date : 13 Oktober 2025

6(2), 97–112.

Rismasari, D. A., & Wikartika, I. (2025). Sosialisasi meningkatkan kesadaran masyarakat dalam mencegah kebocoran data nasabah perbankan digital melalui pesan phishing di era digitalisasi. *Jubaedah: Jurnal Pengabdian dan Edukasi Sekolah (Indonesian Journal of Community Services and School Education)*, 5(1).

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis teknik social engineering sebagai ancaman dalam keamanan sistem informasi: Studi literatur. *JIFTI - Jurnal Ilmiah Teknologi Informasi dan Robotika*, 2(2), 21–30.

Sari, W. P. (2025). Analisis tingkat literasi digital generasi Z dalam penggunaan aplikasi BSI Mobile di Kota Palopo [Skripsi, Institut Agama Islam Negeri Palopo].

Stevani, A. (2025). Strategi komunikasi krisis: Respons perusahaan terhadap skandal personal brand ambassador. *Jurnal Ilmu Komunikasi Andalan*, 8(1), 64–76.

Tannavaro, D. M., & Wiraguna, S. A. (2025). Strategi komunikasi humas dalam krisis siber: Studi kasus BPJS Kesehatan dan Bank Syariah Indonesia. *Kohesi: Jurnal Multidisiplin Saintek*, 7(11), 1–23.

Utomo, N. S. (2015). Manajemen komunikasi eksternal (manajemen komunikasi PT. Semen Indonesia (Persero) Tbk dalam proses pembangunan pabrik semen di Desa Tegaldowo, Kecamatan Gunem, Kabupaten Rembang). *Manajemen Komunikasi Eksternal*, 7(2), 63–67.

Virginia, V. V., Nuha, N. A., Sajidah, L., Krisis, M. I., Relations, P., & Komunikasi, S. (2025). Strategi manajemen isu dan krisis dalam accidental cluster: Analisis strategi SCCT public relations PT Debindo. 10(3), 496–512.

W. Yuspin, A. O. Putri, A. Fauzie, & J. Pitaksantayothin. (2024). Digital banking security: Internet phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Safety and Security Engineering*, 14(6), 1699–1706.

Yulianti, W., & Boer, R. F. (2020). Manajemen krisis public relations dalam menangani penolakan imunisasi measles rubella. *PRofesi Humas Jurnal Ilmiah Ilmu Hubungan Masyarakat*, 4(2), 290.