

STRATEGI KOMUNIKASI DIGITAL BANK BCA DALAM MENSOSIALISASIKAN AMAN TRANSAKSI PERBANKAN UNTUK MENGHINDARI KEJAHATAN *CYBER CRIME*

PENULIS

¹⁾Mohammad Ryan Rhamadhan, ²⁾Alfan Bachtiar, ³⁾Rezzi Nanda Barizki,
⁴⁾Nur Desilawati, ⁵⁾Alamsyah

ABSTRAK

Sosialisasi transaksi perbankan yang aman untuk menghindari kejahatan siber serta mengetahui cara mengatasi kejahatan siber dan menemukan kendala dari strategi yang diterapkan oleh Bank BCA. Subjek penelitian ini adalah staf Bank BCA dan nasabah Bank BCA yang menjadi korban kejahatan siber, karena peneliti ingin mengetahui strategi yang telah dilakukan oleh Bank BCA dan cara pencegahan serta penanganannya. Metode penelitian yang digunakan adalah metode deskriptif kualitatif. Teknik pengumpulan data yang digunakan adalah wawancara mendalam, observasi, dan dokumentasi. Penentuan informan kunci menggunakan teknik purposive sampling. Teknik analisis data yang digunakan adalah reduksi data, penyajian data, dan penarikan kesimpulan. Teknik validitas data menggunakan triangulasi sumber. Hasil penelitian ini mengungkapkan bahwa 7 informan kunci dari staf Bank BCA dan nasabah Bank BCA yang terdampak kejahatan siber menunjukkan pentingnya kesadaran terhadap data pribadi yang bersifat rahasia. Faktor pendukung termasuk peran aktif staf Bank BCA, adanya kampanye "Tolak Dengan Anggun," serta penggunaan media sosial secara bijak. Sementara itu, faktor penghambat berasal dari nasabah yang apatis, kesulitan dalam teknologi, banyaknya nasabah yang sudah berusia lanjut, dan kurangnya pengetahuan. Kesimpulan dari penelitian ini adalah betapa pentingnya strategi digital yang diterapkan oleh Bank BCA dalam menangani dan mengurangi jumlah kasus kejahatan siber di Indonesia, serta upaya Bank BCA untuk meningkatkan infrastruktur keamanan digital dan melindungi data nasabah.

Kata Kunci

Strategi; Komunikasi Digital; Sosialisasi; Bank BCA; *Cyber Crime*

ABSTRACT

The purpose of this research is to determine Bank BCA's digital communication strategy in socializing safe banking transactions to avoid cyber crime and find out how to overcome cyber crime and find out the constraints of the strategy implemented by Bank BCA. The subjects of this study are Bank BCA staff and Bank BCA customers who are victims of cyber crime because researchers want to know what strategies Bank BCA has carried out and how to prevent and overcome them. The research method used is qualitative descriptive method. The data collection techniques used are in-depth interviews, observation and documentation. Key informant determination technique using purposive sampling. The data analysis techniques used are data reduction, data presentation and conclusion. Data validity techniques use source triangulation. The results of this study revealed that 7 key informants from Bank BCA staff and Bank BCA customers affected by cyber crime revealed the importance of awareness of confidential personal data. With supporting factors that include the active role of Bank BCA staff, there is a campaign "Tolak Dengan Anggun" and wisely use social media. As well as inhibiting factors that come from customers who are apathetic, technology stuttering, with many customers still elderly and supported by lack of knowledge. The conclusion in this study is how important the digital strategy implemented by Bank BCA in tackling and reducing the number of cyber crime cases in Indonesia as well as Bank BCA's efforts to improve digital security infrastructure and protect customer data.

Keywords

Strategy; Digital Communication; Socialization; Bank BCA; Cyber Crime

AFILIASI

Prodi, Fakultas
Nama Institusi
Alamat Institusi

¹⁻⁵⁾Program Studi Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik
¹⁻⁵⁾Institut Bisnis dan Informatika (IBI) Kosgoro 1957
¹⁻⁵⁾Jl. Moch. Kahfi II No. 33, Jagakarsa, Jakarta Selatan

KORESPONDENSI

Penulis
Email

Mohammad Ryan Rhamadhan
ryanrhmdhn@gmail.com

LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

I. PENDAHULUAN

Kejahatan di Indonesia saat ini masih menjadi perhatian kita bersama tak terkecuali *cyber crime*. *Cyber crime* menjadi marak karena kecanggihan teknologi saat ini seiring dengan kemajuan tersebut, salah satu dampak negatif yang ditimbulkan yaitu perkembangan kejahatan *cyber crime* yang semakin meningkat. Hal ini ditandai dengan meningkatnya kasus siber dan juga banyaknya serangan siber terhadap sistem dan server di belahan dunia, termasuk di Indonesia. Perkembangan zaman yang berubah menjadi Revolusi Industri 4.0 banyak memberikan pengaruh signifikan terhadap tingkat kejahatan yang semakin berevolusi dan modern. Bahkan, kejahatan konvensional sudah banyak ditinggalkan dan beralih kepada kejahatan yang sifatnya kejahatan dunia maya atau dikenal dengan istilah *cyber crime*. Berdasarkan dari Peta Serangan Siber ke Indonesia per tanggal 15 November 2022, Indonesia menempati urutan ke-1 negara yang paling banyak diserang (sumber: <https://honeynet.bssn.go.id/>).

Pada hakikatnya, kejahatan dunia maya tidak mengenal batasan ruangan. Pelaku melancarkan aksinya hanya mengandalkan jaringan internet dan teknologi yang ada. Hal ini disebabkan karena kejahatan dunia maya, tidak seperti kejahatan tradisional yang dilakukan di satu lokasi tertentu. Namun, dilakukan secara *online* dan sering tidak jelas terkait geografis manapun. Perkembangan teknologi seperti mata pisau yang akan menjadi bermanfaat jika digunakan dengan baik dan bijak namun juga sebaliknya jika dimanfaatkan dengan sangat buruk jika digunakan untuk tindak kejahatan kriminal. Perhatian terhadap kejahatan *cyber crime* tersebut dikarenakan dampak dari adanya *cyber crime* bersifat negatif yang dapat merusak terhadap seluruh bidang kehidupan modern saat ini, oleh karena kemajuan teknologi komputer menjadi salah satu pendukung kehidupan masyarakat nasional mengakibatkan timbulnya banyak korban tidak terkecuali dengan dunia perbankan.

Dalam dunia *cyber crime* perbankan dapat diketahui macam – macam kejahatan dari kegiatan *cyber crime* transaksi perbankan yang memakai alat Internet sebagai basis transaksi yakni sistem layanan kartu kredit dan debit serta layanan perbankan *online* (*online banking*). Korban akibat kejahatan *cyber crime* di bidang perbankan diantaranya para penyimpan dana dan bank yang bersangkutan. Kejahatan perbankan lahir dan tumbuh seiring dengan kemajuan ilmu pengetahuan dan teknologi yang dicapai oleh manusia. Kejahatan tersebut termasuk dalam kategori kejahatan kelas “*elite*”. Dikatakan kelas “*elite*” karena tidak semua orang dapat untuk melakukannya. Dituntut memiliki kemampuan berpikir untuk mencapai hasil yang berlipat ganda. Semakin maju dan berkembang sistem *digital*, akan semakin juga mewarnai bentuk dan corak kejahatan yang akan muncul ke permukaan.

Dalam sistem layanan yang pertama, yang perlu diwaspadai yaitu tindak kejahatan yang dikenal melalui istilah *carding*. Pada prosesnya yaitu pelaku *carding* mendapatkan data kartu *kredit* dan *debit* korban secara tidak sah (*illegal interception*), kemudian menggunakan kartu kredit dan debit tersebut dalam berbelanja di toko *online*. Modus tersebut biasanya terjadi dikarenakan lemahnya sistem pengecekan yang dipakai dalam memastikan identitas pemesan barang di toko *online*. Kegiatan yang kedua yakni perbankan *online*. Modus yang pernah muncul di Indonesia dikenal melalui istilah *typosite* yang memanfaatkan kelengahan nasabah yang salah menyetikkan alamat bank *online* yang ingin diaksesnya. Pelakunya telah mempersiapkan situs palsu yang mirip dengan situs asli bank *online*. Jika ada nasabah yang salah ketik dan masuk ke situs bank palsu tersebut, maka pelaku akan merekam *user ID* serta *password* nasabah tersebut agar dipakai dalam mengakses ke situs yang sebenarnya bertujuan agar mengambil uang nasabah. Dan salah satu tindakan kejahatan yang umum dilakukan adalah pencurian data kartu kredit dan debit, atau yang biasa disebut dengan istilah *phishing* (Nunuk, 2018). Orang atau komplotan yang melakukan *phishing* biasanya mengincar 4 digit nomor di belakang kartu kredit dan nomor *PIN*-nya. Informasi ini kemudian digunakan oleh pelaku untuk bertransaksi atas nama nasabah. terdapat empat teknik yang umum atau sering dilakukan pelaku pencurian data kartu kredit, yaitu pelaku akan menelpon dan mengaku sebagai perwakilan dari pihak Bank atau *surveyor* yang ingin memperbaharui data kartu kredit dan debit. Modus lain yang sering digunakan adalah membuat situs belanja *online* palsu. Karena apabila melakukan pembayaran kartu kredit pada situs *online* yang tidak terpercaya, kemungkinan tujuan mereka adalah mencuri data kartu kredit dan debit. Adapun modus *cyber crime* lainnya yakni “*Skimming*”. *Skimming* sendiri adalah tindakan pencurian informasi kartu baik debit maupun kredit dengan cara menyalin informasi yang terdapat pada *strip magnetik* kartu. *Strip magnetik* kartu adalah garis lebar hitam yang terletak di bagian belakang kartu. *Strip magnetik* ini merupakan tempat tersimpannya informasi mengenai kartu tersebut. Teknik *skimming* dilakukan dengan menggunakan alat penyalin informasi. Umumnya, alat ini ditempelkan pada mesin ATM Bank. Namun juga dapat dilakukan pada mesin *EDC* kartu kredit dengan metode yang sama. Pelaku menggunakan sebuah alat seperti *reuter internet*, yang dapat menciptakan koneksi internet Wi-Fi palsu di *gadget* calon korban. Ketika calon korban telah terkoneksi dengan koneksi ini, si pelaku dapat dengan mudah melihat informasi yang tersimpan dalam *browsing history* korban.

Salah satu perbankan yang ikut memerangi kejahatan *cyber crime* ini adalah PT Bank Central Asia (BCA). PT BCA sendiri terus berupaya untuk meminimalisir kejahatan *cyber crime* ini. Sebab kerugian yang dialami oleh perusahaan dapat berupa pendapatan yang menurun, kerugian nilai pasar dan rusaknya reputasi perusahaan yang nantinya akan berdampak pada hilangnya kepercayaan masyarakat terhadap PT BCA. Dari data Bank BCA Kantor Cabang Pembantu Menara Imperium dalam 5 bulan terakhir kejahatan *cyber crime* perbankan mengalami kenaikan secara terus menerus. Berikut data kasus kejahatan *cyber crime* (*Skimming dan Phishing*) di KCP Menara Imperium periode Bulan Juli - November 2022 dan dapat dilihat pada (tabel 1).

Tabel 1. Kasus Kejahatan *Cyber Crime* Periode Bulan Juli - November 2022 KCP Menara Imperium

No.	Periode Bulan	Kasus Kejahatan <i>Cyber Crime</i>	
		<i>Skimming</i>	<i>Phishing</i>
1	Juli	2 Kasus	2 Kasus
2	Agustus	3 Kasus	5 Kasus
3	September	5 Kasus	8 Kasus
4	Oktober	7 Kasus	20 Kasus
5	November	8 Kasus	25 Kasus

Sumber: Olahan Peneliti, 2022

Dalam tabel tersebut dapat dikatakan bahwa, dalam periode bulan Juli sampai dengan bulan Agustus untuk kejahatan *cyber crime* secara terus menerus mengalami lonjakan kasus yang signifikan dan jika diabaikan akan berakibat fatal karena menyangkut dengan profil nasabah seperti data nasabah, dan dana yang dimiliki oleh nasabah. Dalam hal ini, penyedia layanan perbankan yakni PT BCA bertanggung jawab untuk dan mengembangkan keamanan yang berkelanjutan dan sistematis demi mewujudkan ekosistem *digital* yang aman. Sementara itu, nasabah juga perlu waspada untuk ikut membantu melindungi data dan dana miliknya agar tidak disalahgunakan oleh oknum yang tidak bertanggung jawab. Salah satu faktor penting untuk mewujudkan hal ini adalah adanya edukasi yang terintegrasi dan berkelanjutan agar dapat menjangkau masyarakat dengan memiliki pemahaman akan modus kejahatan *cyber crime*. Modus kejahatan *digital* memang akan terus berkembang tetapi kita dapat meminimalisir dengan pengetahuan dan tahapan edukasi yang terus dilakukan oleh penyedia jasa layanan perbankan khususnya PT Bank Central Asia. BCA telah menerapkan strategi untuk memastikan transaksi para nasabahnya aman dan lancar. Namun, disisi lain BCA juga terus mengedukasi para nasabah setianya untuk ikut serta dalam menjaga data pribadi seperti tidak memberikan *PIN*, tidak mengisi sarana *link* atau situs yang di berikan oleh orang lain, kode *OTP*, informasi rahasia dan data pribadi kepada pihak yang tidak berkepentingan.

Dari uraian diatas, penulis tertarik untuk melakukan penelitian dan menganalisis terkait dengan strategi komunikasi *digital* dalam mengedukasi nasabah untuk menghindari kejahatan *cyber crime*. Oleh karena itu, penulis bermaksud untuk membuat penelitian berjudul “Strategi Komunikasi Digital Bank BCA dalam Mensosialisasikan Aman Transaksi Perbankan untuk Menghindari Kejahatan *Cyber Crime*”.

II. METODE PENELITIAN

Pendekatan penelitian yang digunakan pada penelitian ini adalah penelitian kualitatif. Penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian. Seperti halnya perilaku, persepsi, motivasi dan tindakan. Dengan cara ini deskripsi dalam bentuk kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode alamiah. Penelitian kualitatif adalah strategi *inquiry* yang dilakukan untuk mencari makna, pengertian, konsep yang digunakan, karakteristik yang terbangun, gejala yang ditimbulkan, simbol-simbol serta pemahaman secara jelas tentang suatu fenomena yang bersifat alami dan *holistic*, mengutamakan kualitas, menggunakan cara-cara yang efektif dan disajikan dalam bentuk naratif. (Yusuf, 2014)

Adapun metode penelitian yang digunakan dalam penelitian ini yaitu metode deskriptif. Metode deskriptif memberikan gambaran atau mendeskripsikan dengan mengumpulkan data kemudian dianalisis dengan deduktif. Peneliti menggunakan metode deskriptif karena peneliti ingin mendapatkan data yang mendalam didasari oleh fakta-fakta yang ditemukan pada saat penelitian di lapangan.

Penelitian deskriptif timbul karena suatu peristiwa yang menarik perhatian peneliti tetapi belum ada kerangka teoritis yang menjelaskannya. Metode deskriptif ini memfokuskan pada observasi di lapangan dan suasana ilmiah sehingga peneliti melakukan pengamatan secara langsung pada lokasi penelitian, data yang dihasilkan yaitu berupa kata-kata, gambar yang berasal dari wawancara, catatan lapangan, foto dan dokumen yang relevan terhadap masalah yang diteliti. (Rakhmat, 2013)

Teknik pengumpulan data ialah langkah yang primer dalam proses penelitian berlangsung, karena tujuan utama dari penelitian adalah mendapatkan data yang valid dan sah. Berkaitan dengan hal itu pada bagian ini jenis datanya dibagi kedalam kata-kata dan tindakan, sumber data tertulis, foto dan statistik. Berikut merupakan teknik-teknik pengumpulan data yang dilakukan yakni: Wawancara yang mendalam Wawancara dapat didefinisikan sebagai interaksi bahasa yang berlangsung antara dua orang dalam situasi saling berhadapan salah seorang yaitu melakukan wawancara meminta informasi kepada orang yang diteliti dengan berputar pendapat. (Emzir, 2014). Dalam penelitian ini, wawancara dilakukan untuk memperoleh data dan sumber informasi secara langsung berupa informasi mengenai kejahatan *cyber crime* khususnya kejahatan perbankan di KCP BCA Menara Imperium.

Observasi, Menurut (Karl Weick, 2012) mendefinisikan observasi sebagai pemilihan, pengubahan, pencatatan, dan pengodean serangkaian perilaku dan suasana yang berkenaan sesuai dengan tujuan-tujuan empiris. Observasi yang dilakukan pada penelitian ini bersifat partisipan dimana peneliti melakukan pengamatan langsung ditempat penelitian yang berkesinambungan dengan keseharian informan.

Studi dokumentasi, Menurut (Sugiyono, 2015) Dokumentasi adalah suatu cara yang digunakan untuk memperoleh data dari informasi dalam bentuk buku, arsip, dokumen, tulisan angka dan gambar yang berupa laporan serta keterangan yang dapat mendukung penelitian. Studi dokumentasi merupakan salah satu cara dimana peneliti kualitatif dapat memvisualisasikan perspektif subjek melalui materi tertulis atau dokumen lain yang dihasilkan langsung oleh peneliti. Dokumentasi yang dilakukan dalam penelitian ini adalah pengambilan gambar atau foto ketika observasi.

Teknik penentuan informan, Informan merupakan seseorang yang memberikan informasi yang dicari oleh peneliti, informan bisa juga dikatakan sebagai sumber data yang sangat dibutuhkan oleh peneliti. Pemilihan informan pada penelitian ini didasari pada kriteria yang sudah ditentukan oleh peneliti yang biasa disebut dengan *Purposive Sampling*. Teknik penentuan informan menggunakan *Purposive Sampling* adalah teknik pengambilan sampel sumber data yang didasarkan dengan pertimbangan tertentu yang berkaitan dengan studi kasus yang diteliti dan tujuan peneliti. (Sugiyono, 2013). Dimana kriteria tersebut dibuat agar penelitian yang dilakukan oleh peneliti tepat sasaran dan tidak bertele-tele.

Teknik analisis data merupakan langkah yang dilakukan oleh seorang peneliti untuk mencari, menata dan merumuskan kesimpulan-kesimpulan secara sistematis dari catatan hasil wawancara, observasi dilapangan, studi pustaka serta dokumentasi. Aktivitas dalam analisis data, yaitu pengumpulan data, reduksi data, penyajian data, dan penarikan kesimpulan dan verifikasi, yang disebut dengan Analisis Data Model Miles and Huberman (Sugiyono, 2019).

Pengumpulan data dalam penelitian kualitatif pengumpulan data dengan observasi, wawancara mendalam, dan dokumentasi atau gabungan ketiganya (triangulasi). Pengumpulan data dilakukan sehari-hari, mungkin berbulan-bulan, sehingga data yang diperoleh akan banyak. Pada awal peneliti melakukan penjelajahan secara umum terhadap situasi sosial/obyek yang diteliti, semua yang dilihat dan didengar direkam semua. Dengan demikian peneliti akan memperoleh data yang sangat banyak dan sangat bervariasi. Reduksi Data menurut (Sugiyono, 2019), data yang diperoleh dari lapangan cukup banyak, untuk itu maka perlu dicatat secara teliti dan rinci. Seperti yang telah dikemukakan, semakin lama peneliti ke lapangan, maka jumlah data akan semakin banyak, kompleks dan rumit, sehingga untuk itu perlu segera dilakukan analisis data melalui reduksi data. Mereduksi data berarti merangkum, memilah dan memilih hal-hal yang pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya. Kemudian dengan demikian data yang telah direduksi akan memberikan gambaran yang lebih jelas, dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya, dan mencarinya bila diperlukan.

Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah bila tidak ditemukan bukti-bukti yang kuat yang mendukung pada tahap pengumpulan data berikutnya. Kemudian apabila kesimpulan yang dikemukakan pada tahap awal, didukung oleh bukti-bukti yang valid dan konsisten saat peneliti kembali ke lapangan mengumpulkan data, maka kesimpulan yang dikemukakan merupakan kesimpulan yang kredibel. Dengan demikian kesimpulan dalam penelitian kualitatif merupakan temuan baru yang belum pernah ada.

III. HASIL DAN PEMBAHASAN

Pembahasan hasil penelitian diperlukan untuk merangkum kajian yang di dapatkan dari hasil penelitian, peneliti berupaya objektif Menyusun pembahasan penelitian dengan *focus* pada masalah penelitian, konsep dan teori yang di gunakan dan hasil dari wawancara narasumber, Adapun hasil rangkuman penelitian terkait dengan judul penelitian ini yaitu strategi komunikasi *digital* Bank BCA dalam mensosialisasikan aman transaksi perbankan untuk menghindari kejahatan *cyber crime*.

3.1 Konsep Strategi Komunikasi *Digital Bank BCA*

Strategi yang diterapkan oleh Bank BCA sudah dilakukan secara masif. Hal tersebut ditinjau dari pernyataan informan yang disampaikan dalam wawancara. (Ahmad, 2020) strategi adalah prosedur yang sistematis dalam melaksanakan rencana yang komprehensif dan berjangka panjang untuk mencapai tujuan. (Munarika, 2018) juga mengungkapkan bahwa strategi adalah suatu proses penentuan rencana para pemimpin puncak yang berfokus pada tujuan jangka panjang organisasi, disertai penyusunan suatu cara atau upaya bagaimana agar tujuan tersebut dapat dicapai. Dari strategi yang sudah ditetapkan dalam hal ini perbankan sebagai penyedia jasa bermaksud untuk memberikan sosialisasi secara menyeluruh, agar terciptanya transaksi yang aman dan cepat tanpa ada pihak manapun yang dirugikan. Bank BCA selalu berkomitmen untuk selalu memberikan pelayanan terbaik kepada nasabahnya. (Kasmir, 2014) Bank dikenal sebagai lembaga keuangan yang kegiatan utamanya menerima simpanan giro, tabungan, dan deposito. Bank BCA sebagai penyedia jasa selalu ingin memberikan informasi kepada nasabah setianya. Pada tahap ini, BCA selalu berkomitmen agar apapun berita atau informasi yang berkembang dimasyarakat khususnya perbankan dapat disosialisasi dengan baik melalui cara konvensional yakni datang langsung ke cabang maupun *digital (website atau social media)*. Sosialisasi akan dilakukan secara terus menerus agar terciptanya pelayanan perbankan yang profesional. Dalam hal ini, sosialisasi terhadap kejahatan perbankan yang menurut pandangan kita sudah sangat meresahkan dan merugikan banyak pihak. Sosialisasi merupakan proses penyampaian suatu pesan oleh seseorang kepada orang lain untuk memberi tahu atau mengubah sikap, pendapat, perilaku baik langsung maupun tidak langsung (Agustin, 2014). Sosialisasi yang dilakukan sudah secara menyeluruh guna mengurangi angka kejahatan di perbankan.

Dalam sosialisasinya Bank BCA sudah melakukan berbagai cara yakni sosialisasi dengan teknologi *digital* untuk menjangkau seluruh nasabahnya. Menurut, (Musnaini, Suherman, Wijoyo, & Indrawan 2020) *digital* merupakan sebuah metode yang kompleks dan fleksibel yang membuatnya menjadi sesuatu yang pokok dalam kehidupan manusia. Teknologi *digital* inilah yang dimanfaatkan oleh Bank BCA untuk menyebar luaskan informasi dan edukasi kepada seluruh nasabahnya. Perlu diketahui untuk fungsi dari *digital* itu sendiri terjadinya efisiensi tenaga dan waktu, dengan adanya pemanfaatan ini Bank BCA akan lebih efisien untuk mensosialisasikan tentang informasi yang ingin mereka sebar.

3.2 Fenomena Kasus Kejahatan *Cyber Crime*

Saat ini perkembangan digital sangat berkembang pesat. Pengaruh ini diikuti juga dengan perkembangan di sistem perbankan, namun pada saat perkembangan teknologi *digital* sedang mengalami tren yang meningkat bagi penggunaannya tidak berbanding lurus dengan kelemahan *digital*-nya. Unsur kelemahan ini malah dijadikan sebagai alat memeras, mengelabui dan mengintimidasi kejahatan pada perbankan. Kejahatan Perbankan adalah bentuk perbuatan yang telah diciptakan oleh undang-undang perbankan yang merupakan larangan dan keharusan, misalnya larangan mendirikan bank gelap dan pembocoran rahasia bank (Nunuk, 2018). Kejahatan perbankan sendiri mempunyai berbagai macam jenisnya. Di penelitian ini, peneliti akan membagi dua jenis kejahatan perbankan melalui media *cyber crime* yakni *skimming* dan *phishing*. Karena dua tipe kejahatan inilah yang sedang *trend* bagi para pelaku. *Skimming* menurut (sumber: <https://ojk.go.id/>) adalah tindakan pencurian informasi kartu debit atau kartu kredit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu debit atau kartu kredit secara ilegal.



Gambar 1. Kejahatan Perbankan *Skimming*

Sumber: <https://ojk.go.id/>

Pada kejahatan *skimming* ini pelaku melakukan dengan teknik *skimming* yang menggunakan alat dan ditempelkan pada mulut mesin ATM (tempat masuk kartu ATM) dengan alat yang dikenal atau disebut *skimmer*. Modus operasi yang dilakukan oleh pelaku kejahatan dengan *mengcloning* (menduplikat) data dari *magnetic stripe* yang terdapat pada kartu ATM milik nasabah. Selain di mesin ATM, tindak kejahatan *cyber crime skimming* juga bisa dilakukan di mesin *Electronic Data Capture* (EDC) yang biasanya kita dapat jumpai di kasir-kasir atau *outlet* pembayaran pada toko perbelanjaan. Ada dua metode dalam melakukan *skimming* pada mesin EDC yaitu dengan menyematkan alat *skimmer* khusus pada mesin EDC dan yang kedua adalah dengan metode agak lebih rumit yaitu *wire tapping*. Metode ini bertujuan untuk menyadap saluran komunikasi data antara koneksi mesin EDC dan mesin kasir menuju bank atau lembaga keuangan yang dituju.

Dalam hal ini, Bank BCA sudah menyiapkan strategi *digital* nya dengan membuat poster *digital* yang ada *website*, maupun informasi yang sering kita lihat di mesin ATM. Untuk setidaknya mencegah agar para nasabah setia BCA tidak terkena modus kejahatan *cyber crime* ini.



Gambar 2. Tips Terhindar Dari Kejahatan Perbankan *Skimming*

Sumber: <https://bca.co.id/>

Berikutnya modus kejahatan *cyber crime phishing* (Sumber : <https://ojk.go.id/>) adalah salah satu ancaman kejahatan yang dilakukan dengan cara mencuri data penting orang lain, termasuk antara lain data bank seperti nomor rekening, data ATM seperti nomor kartu dan *PIN*, serta data kartu kredit seperti nomor kartu dan *PIN*. Data-data yang diincar biasanya berupa tanggal lahir, username/user ID dan kata sandi (*password*), *PIN* ATM, nomor kartu kredit/debit, masa berlaku kartu kredit/debit, *CVV/CVC* (3 angka di belakang kartu kredit), *OTP* transaksi hingga nomor kartu kependudukan (KTP atau *passport*). Jenis kejahatan *phishing* ini sedang trend atau naik daun karena untuk kasus kejahatan *cyber crime* ini yang paling mudah karena para pelaku ini melihat kegiatan para nasabah yang sedang *happening* itu apa. Sebagai contoh yang baru-baru ini kita ketahui dengan pelaku mengirim *link* ke sosial media kita seperti *whatsapp* atau *via email*, dari hasil wawancara kepada informan yang bernama Tiara Afisyah. Ia mengaku jika terkena modus kejahatan *phishing* itu dari adanya yang mengaku-ngaku sebagai kurir paket dimana memang trend untuk pengiriman paket ataupun *cash on delivery* (*COD*) *via marketplace* sedang menjamur. Hal ini yang memang dimanfaatkan oleh pelaku kejahatan *phishing* untuk melancarkan aksi kejahatannya. Karena memang banyak dari nasabah yang merasa memesan paket lalu pelaku atau penipu melakukan persuasi atau ajakan untuk mengklik *link* yang tersedia pada kolom chat. Jika apabila nasabah sudah mengklik *link* sudah dipastikan untuk file data-data perbankan dan data pribadi yang sifatnya rahasia berhasil dicuri oleh pelaku. Dalam hal ini, Bank BCA tidak tinggal diam, BCA sudah melakukan kegiatan sosialisasi terhadap kejahatan yang sedang *booming* di masyarakat, dari nasabah yang datang ke cabang maupun para staff BCA yang selalu menyebarluaskan informasi dan edukasi kepada nasabah setia BCA melalui *handphone* pribadinya. Tidak hanya itu Bank BCA juga menyoroti ciri-ciri bagi pelaku kejahatan *cyber crime phishing* yakni : perintah mengisi data sensitif dan bersifat rahasia, menggunakan identitas palsu, memberi tautan atau file palsu, email yang bersifat rayuan bahkan ancaman, dan korban *phishing* yang tidak spesifik. Mencermati hal tersebut Bank BCA sudah melakukan strategi *digital* agar nasabah aman untuk bertransaksi. Bank BCA juga membuat sebagai cara

sosialisasi dengan poster *digital* dengan langkah-langkah atau antisipasi bagi para nasabah setianya agar dapat memahami dan terhindar dari kejahatan *cyber crime* jenis *phishing*. Berikut langkah-langkah yang mudah diterapkan oleh nasabah Bank BCA.

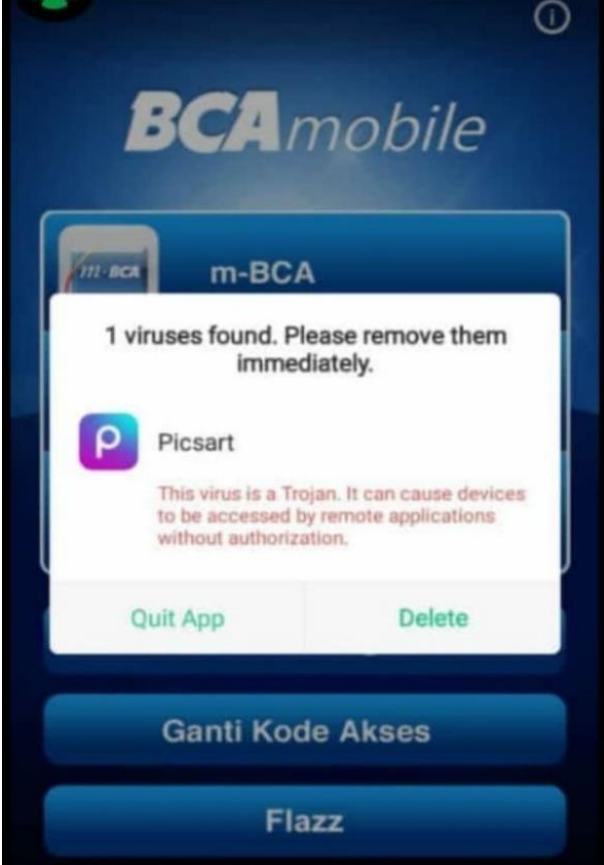



Gambar 3. Tips Terhindar dari Kejahatan *Cyber Crime Phishing*

Sumber: <https://bca.co.id/>

Selain itu, kejahatan *cyber crime phishing* juga sudah berkembang pesat sedemikian rupa untuk mencari celah agar nasabah BCA terjerat akan kasus kejahatan ini. Baru-baru ini berkembang modus kejahatan *cyber crime phishing* yang menginformasikan kepada nasabah BCA bahwa adanya kenaikan tarif transfer dan cara mudah mendapatkan fasilitas BCA Prioritas. Dalam hal ini, Bank BCA menuturkan bahwa yang diinformasikan kepada nasabah BCA adalah tidak benar dan termasuk kedalam tindak kejahatan *cyber crime phishing*.

Berdasarkan temuan hasil observasi peneliti terbaru dalam kejahatan *cyber crime phishing*, ditemukannya modus penipuan yang lebih berbahaya. Karena pada modus kejahatan ini, para *hacker* sudah menyusup pada aplikasi *e-channel* Bank BCA yakni *mobile banking*. Masyarakat khususnya nasabah setia BCA dihimbau untuk selalu berhati-hati setiap kali menggunakan aplikasi *mobile banking* dan tidak mengklik tombol apapun jika sudah ada modus *link* yang bermuatan jika *handphone* nasabah sudah terserang *virus trojan*. Berikut gambar modus penipuan terbaru dengan menggunakan *mobile banking*.





INFORMASI

Topik/ Isu : Pop Up di BCA Mobile
Atribusi Narasumber : Hera F. Haryn, EVP Corporate Communication & Social Responsibility

Jakarta, 24 Juli 2023 - Sehubungan dengan informasi yang beredar di sosial media terkait tampilan pop up peringatan virus di aplikasi BCA mobile, dapat kami sampaikan bahwa nasabah agar berhati-hati atas hal tersebut. Kami menghimbau agar nasabah **TIDAK MELAKUKAN KLIK APAPUN** yang muncul di pesan tersebut.

BCA senantiasa mengimbau nasabah setia untuk selalu waspada saat melakukan install aplikasi di luar PlayStore, AppleStore atau store resmi lainnya, serta melakukan update software perangkat smartphone terbaru.


BCA juga senantiasa mengedepankan keamanan dan kenyamanan nasabah dalam bertransaksi. Kami kembali menghimbau kepada seluruh nasabah BCA untuk **TIDAK MEMBERIKAN DATA YANG BERSIFAT RAHASIA** kepada pihak manapun (termasuk kerabat, orang terdekat), seperti:

- Personal Identification Number (PIN)
- One Time Password (OTP)
- Password
- Response KeyBCA
- Card Verification Code (CVC) atau Card Verification Value (CVV)

Pastikan juga untuk mendapatkan informasi hanya dari channel resmi BCA yaitu:

- ✓ Aplikasi Halo BCA
- ✓ No Resmi Halo BCA 1500888 (tanpa 021, +0621, atau tambahan lainnya)
- ✓ WhatsApp: Bank BCA 08111500998 (ada centang hijau)
- ✓ Instagram: @goodlifebca (sudah centang biru)
- ✓ Website: www.bca.co.id

Demikian disampaikan.
Terima kasih



PT BANK CENTRAL ASIA TBK
 Group Corporate Communication and Social Responsibility - CSR
 Corporate Communication
 Alamat : Jl. MH Thamrin No.1, Menara BCA Lt. 22, Jakarta 10310
 Telepon : (021) 2358-8000
 Fax : (021) 2358-8339
 E-mail : corcom_bca@bca.co.id

Gambar 4. Modus Penipuan Terbaru Melalui Mobile Banking

Sumber: <https://bca.co.id>

Dengan adanya himbauan seperti pada gambar diatas, diharapkan nasabah Bank BCA selalu *aware* dengan rekeningnya dan peringatan untuk berhati-hati saat menggunakan *mobile banking*. Berhati-hati dengan modus *link* berbahaya adalah suatu hal yang terpenting, terutama dalam era di mana teknologi semakin berkembang. Bank BCA juga sudah mengeluarkan himbauan yang bisa kita akses melalui *website* atau sarana *social media* resmi dari Bank BCA penting untuk selalu memverifikasi sumber informasi sebelum mempercayai atau menyebarkan informasi tersebut. Dapat diketahui, himbauan tersebut bisa diakses melalui media sosial resmi Bank BCA seperti *website* BCA (www.bca.co.id), *Whatsapp* resmi Bank BCA yang bertanda centang hijau, Instagram (@GoodLifeBCA), Twitter (@HaloBCA), dan TikTok (@BankBCA).

3.3 Kampanye Sosial untuk Mengurangi Kejahatan *Cyber Crime*

Berdasarkan dari hasil penelitian, sosialisasi ini akan terus digencarkan oleh Bank BCA dapat kita ketahui bahwa akhir-akhir ini Bank BCA sedang mengampanyekan pencegahan kejahatan *cyber crime* dengan menggandeng artis ternama di Ibukota yakni Anggun C. Sasmi. Anggun sebagai *brand ambassador* Bank BCA untuk mengajak seluruh nasabah setia BCA agar selalu *aware* terhadap data-data pribadi yang sifatnya rahasia seperti: nomor kartu ATM, *PIN*, kode *OTP*, *CVV/CVC*, kode respons *KeyBCA appli* 1 dan 2 yang dapat diketahui oleh penipu.

(Kotler dan Amstrong, 2014) *brand ambassador* merupakan individu yang akan menyebarkan informasi mengenai suatu produk dari suatu perusahaan. (Shimp, 2014) juga mengatakan bahwa *brand ambassador* adalah seseorang yang dapat mendukung iklan, atau yang dikenal sebagai bintang iklan, yang akan mendukung suatu produk yang akan diiklankan.

Sebagai *brand ambassador* Bank BCA, Anggun C. Sasmi memiliki peran yang sangat penting dalam kampanye pencegahan *cyber crime*. Dengan popularitasnya sebagai artis di Ibukota, Anggun dapat menjadi figur yang diidolakan oleh orang banyak, termasuk calon nasabah dan nasabah Bank BCA. Sebagai akibatnya, pesan-pesan yang disampaikan oleh Anggun dapat mudah diterima dan direspons oleh khalayak. Melalui kampanye dan kolaborasi yang melibatkan Anggun sebagai *brand ambassador*, diharapkan pesan-pesan ini dapat lebih luas disampaikan kepada masyarakat Indonesia dan kesadaran tentang keamanan *cyber crime* semakin meningkat.

Dengan adanya kolaborasi tersebut, maka masyarakat dihimbau agar selalu mengingat pesan atau tagline yang disampaikan oleh Anggun. Makna dari tagline ini mengambil dari nama kata Anggun yang memiliki arti yakni tingkah laku dan gaya yang apik. Diharapkan masyarakat selalu bersikap Anggun untuk semua modus kejahatan *cyber crime*.

Menurut (Ainurrofiqin, 2021) *tagline* adalah suatu kalimat singkat yang dibuat oleh suatu perusahaan untuk menjelaskan mengenai makna tertentu dan juga memosisikan merek sehingga akan memiliki suatu perbedaan dengan merek yang lainnya. Mengacu pada kepada kampanye yang dibuat oleh Bank BCA, kampanye tersebut adalah “*Tolak Dengan Anggun*”. Cara paling mudah dan mendasar dari kasus kejahatan *cyber crime* ini adanya seni untuk menolak dengan kata lain hal tersebut dapat mencegah kita dari tindak kejahatan *cyber crime*.



Gambar 5. Tagline Tolak Dengan Anggun

Sumber: <https://bca.co.id/>

Kampanye yang dilakukan oleh Bank BCA ini adalah wujud nyata dimana sudah banyak sekali keresahan yang dirasakan oleh nasabah BCA. Merespons keresahan yang dirasakan oleh nasabah melalui kampanye yang nyata, itu menunjukkan tanggapan dan keseriusan dari pihak Bank BCA dalam menghadapi masalah tersebut. Menurut (Rogers dan Storey, 2018) kampanye merupakan serangkaian tindakan komunikasi yang terencana dengan menciptakan efek tertentu kepada sejumlah besar khalayak yang dilakukan secara berkelanjutan pada kurun waktu tertentu.

Bank BCA juga telah menerapkan keamanan sistem yang maksimal, namun Bank BCA juga butuh bantuan dari nasabah setianya untuk sama-sama menolak dengan Anggun dan dapat dipastikan jika ada seseorang yang minta nomor kartu ATM, PIN, Kode *OTP*, *CVV/CVC*, kode respons *KeyBCA appli* 1 dan 2 *Tolak Dengan Anggun* karena itu sudah pasti unsur tindak kejahatan *cyber crime*. Dengan mengikuti langkah-langkah keamanan diatas dan meningkatkan kesadaran tentang praktik keamanan *cyber crime*, nasabah dapat memberikan kontribusi positif dalam menjaga keamanan akun mereka dan membantu Bank BCA menjalankan operasi dengan lebih aman. Dalam prosesnya, tindakan kejahatan *cyber crime* merupakan ancaman yang serius bagi nasabah bank BCA dan institusi keuangan lainnya. Bank BCA seperti bank-bank lainnya, biasanya memiliki sistem dan tim penanggulangan yang berfungsi untuk menghadapi ancaman kejahatan *cyber crime* dan membantu nasabah yang menjadi korban *cyber crime*.

3.4 Cara Penanggulangan dan Kendala yang Dihadapi Bank BCA

Peneliti juga menemukan bahwa adanya unsur penanggulangan apabila nasabah Bank BCA menjadi korban tindak kejahatan *cyber crime*. Menurut (Suryo Guritno, 2017) penanggulangan adalah upaya yang dilaksanakan untuk mencegah, menghadapi, atau mengatasi suatu keadaan mencakup aktivitas preventif dan sekaligus berupaya untuk memperbaiki perilaku seseorang yang telah dinyatakan bersalah dengan kata lain upaya penanggulangan dapat dilakukan secara preventif.

Dari hasil wawancara kepada informan yang bernama Fellisia Dwi Anggraini bahwa tindak lanjut dari penanggulangan korban kejahatan *cyber crime* ialah dengan cara membuat laporan kejadian terlebih dahulu kepada Halo BCA. Pihak Bank BCA juga menekankan bahwa tidak menjanjikan dana nasabah tersebut bakal kembali. Karena pihak Bank BCA terlebih dahulu melakukan analisa dan tindakan investigasi apa memang murni dari pihak Bank sebagai penyedia jasa yang melakukan kesalahan atau dari pihak nasabah. Bank BCA sebagai penyedia jasa perbankan selalu memberikan solusi yang terbaik untuk para nasabahnya serta di *reminder* kembali kepada nasabah agar selalu berhati-hati dalam bertransaksi agar tidak terulang kembali kasus-kasus kejahatan *cyber crime*. Dapat diketahui, kasus kejahatan *cyber crime* masih menjadi momok bagi Bank BCA disebabkan oleh banyaknya faktor kendala atau penghambat terjadinya proses sosialisasi.

Dalam proses sosialisasi kejahatan *cyber crime* didapatkan juga bahwa kendala atau penghambat yang dialami oleh para staff Bank BCA. Menurut (Kurniawan Budi, 2017) kendala adalah suatu metode yang digunakan untuk melakukan peningkatan secara terus menerus dalam aktivitasnya proses ini harus diulangi secara terus menerus sampai adanya perbaikan. Hal ini diungkapkan oleh informan bahwa masih banyak nya masyarakat yang belum sadar dan apatis betul penting data-data pribadi sifatnya rahasia didukung juga tingkat pemahaman akan *social media*. Menurut (Andi Riswandi, 2017) apatis adalah keadaan ketidakpedulian, di mana seseorang individu tidak menanggapi rasangan emosional, sosial maupun fisik.

Bank BCA selalu menekankan untuk lebih *aware* terhadap rekening nasabah masing-masing agar terhindar dari tindak kejahatan *cyber crime* serta ditambah yakni para pemilik rekening di tahap lanjut usia atau manula yang rentan sekali menjadi korban karena banyak hal teknologi *digital* yang kurang mereka pahami. Mengingat bahwa tindak kejahatan *cyber crime* semakin canggih dan beragam penting bagi semua nasabah, terutama mereka yang rentan terhadap penipuan atau kejahatan *cyber crime*. Sosialisasi dan perlindungan yang tepat akan membantu para nasabah untuk lebih bijaksana dalam bertransaksi secara *digital* dan melindungi aset serta informasi pribadi mereka dari serangan kejahatan *cyber crime*.

Bank BCA selalu berkomitmen untuk selalu mensosialisasikan serta mengedukasi para nasabahnya agar tidak menjadi korban kejahatan *cyber crime*. Dengan melakukan langkah-langkah ini, Bank BCA dapat membantu para nasabahnya menjadi lebih sadar dalam menghadapi ancaman kejahatan *cyber crime*, sehingga mereka dapat lebih melindungi data-data pribadi dan finansial secara efektif. Dalam hal ini, Bank BCA dapat berperan aktif dalam melindungi nasabahnya dari ancaman kejahatan *cyber crime* dan menciptakan lingkungan perbankan yang lebih aman dan terpercaya. Kesadaran dan pendidikan yang baik akan menjadi kunci dalam mengurangi tingkat keberhasilan kejahatan *cyber crime* dan pastinya melindungi kepentingan nasabah.

IV. KESIMPULAN

Strategi komunikasi digital yang dilakukan oleh Bank BCA adalah sosialisasi digital melalui *social media* seperti Website (www.bca.co.id), Whatsapp resmi Bank BCA, Instagram (@GoodLifeBCA), Twitter (@HaloBCA), dan TikTok (@BankBCA). Kemudian kampanye sosial secara *digital* dengan menarik *brand ambassador* yang diperkuat oleh *tagline* "Tolak Dengan Anggun" kampanye dan sosialisasi tersebut dilakukan secara *digital*. Serta didukung oleh loyalitas karyawan Bank BCA melalui *gadget* pribadi dengan rutin untuk meng-*update* status dan melakukan *personal chat* kepada para nasabahnya.

Faktor pendukung dan faktor penghambat dari strategi komunikasi *digital* Bank BCA dalam mensosialisasikan aman bertransaksi perbankan adalah dengan meningkatkan kesadaran masyarakat dan nasabah akan pentingnya data-data pribadi yang bersifat rahasia dengan bijak dalam menggunakan *social media*. Langkah tersebut juga didukung oleh peran aktif para staff BCA yang selalu memberikan sosialisasi terhadap kejahatan *cyber crime*. Sedangkan untuk faktor penghambatnya adalah masih banyaknya nasabah yang bersikap apatis serta nasabah yang sudah memasuki lanjut usia dengan didasari oleh kurangnya ilmu pengetahuan akan pentingnya menjaga data-data pribadi, ditambah dengan gagapnya teknologi yang semakin hari semakin berkembang.

Penelitian ini menggarisbawahi betapa pentingnya strategi *digital* yang diterapkan oleh Bank BCA dalam menanggulangi dan menekan jumlah kasus kejahatan *cyber crime* di Indonesia. Penelitian ini juga menyoroti bahwa upaya Bank BCA untuk meningkatkan infrastruktur keamanan *digital* dan melindungi data nasabahnya, pendekatan proaktif yang diambil oleh bank ini juga telah membantu mencegah serangan kejahatan *cyber crime* dan melindungi informasi keuangan serta data pribadi nasabah.

REFERENSI

- Ahmad. (2020). *Manajemen Strategis*. Makassar: Nass Media Pustaka
- Agustin, Rinny. (2014). *Persepsi Masyarakat Tentang Sosialisasi Bahaya Narkoba di Kelurahan Sidomulyo*. Samarinda: Jurnal Komunikasi
- Cindya Yunita Pratiwi, RR. Roosita Cindrasih, dkk. (2021). *Strategi Komunikasi Digital PT Gojek Indonesia Dimasa Pandemi Covid - 19*
- Dendawijaya. (2013). *Manajemen Perbankan*
- Didik Hariyanto. (2021). *Pengantar Ilmu Komunikasi*
- Edi Suryadi. (2018). *Strategi Komunikasi*. Bandung
- Effendy, Onong Uchjana. (2013). *Ilmu, Teori dan Filsafat Komunikasi*. Bandung: Citra Aditya Bakti Ena Sukmana. (2015). *Digitalisasi Pustaka*. Bandung
- Gita Wideasanty, I. (2018). *Strategi Manajemen Komunikasi Mempertahankan Reputasi*. Jakarta: Inter Komunika
- Hermawan, R. (2015). *Kesiapan Aparatur Pemerintah Dalam Menghadapi Cybercrime Di Indonesia*
- Indrajit, Richardus Eo. (2014). *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*. Yogyakarta: Graha Ilmu
- Jurnalis J.Hius ST. (2014). *Mengenal dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari - Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku*. Banda Aceh: Prosiding SNIKOM
- Kasmir. (2014). *Bank dan Lembaga Keuangan Lainnya*. Jakarta: Rajagrafindo Persada Maskun. (2013). *Kejahatan Cyber Crime Suatu Pengantar*. Jakarta: Prenata Media Group
- Muri Yusuf. (2014). *Metode Penelitian Kuantitatif, Kualitatif dan Penelitian Gabungan*. Jakarta: Kencana Nasrullah, Rulli. (2015). *Media Sosial*. Bandung: PT Remaja Rosdakarya
- Nunuk Sulisrudatin. (2018). *Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit*
- Retraningrum, M.A. (2017). *Perilaku Penemuan dan Pemanfaatan Informasi Di Kalangan Hacker*. Surabaya: Universitas Airlangga
- Rogers, Storey. (2018). *Communication Campaign*. New Burry Park
- RR Ponco Dewi Karyaningish. (2018). *Pengantar Ilmu Komunikasi*. Yogyakarta Sugiyono. (2017). *Metode Kuantitatif, Kualitatif*. Bandung: Indobesia IKPI Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif*. Bandung: Alfabeta
- Widodo. (2013). *Memerangi Cybercrime: Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*. Yogyakarta: Aswaja Pressing
- Wiryanto. (2014). *Pengantar Ilmu Komunikasi*. Jakarta: Grasindo Persada