Volume 5 Nomor 2
Agustus 2022: 220-243

Jurnal Riset Komunikasi
JURKOM

P-ISSN: 2615-0875
E-ISSN: 2615-0948

Komunikasi Termediasi Penipuan dengan Modus *Business Email Compromise*

Tri Andriyanto
Universitas Indonesia
Email: tri.andriyanto11@ui.ac.id

Diterima : 06 Juli 2022 Disetujui : 04 Agustus 2022 Diterbitkan : 12 Agustus 2022

Abstrak

Business Email Compromise (BEC) menjadi modus baru kejahatan siber dalam bentuk email phishing kepada target individu atau korporasi yang dituju guna meraih keuntungan finansial. Artikel ini membahas konsep BEC dalam lingkup komunikasi termediasi dan komunikasi persuasi dari pelaku kepada korban dan dikaitkan dengan teori Computer-Mediated Communication dan Model Kemungkinan Elaborasi. Metode penelitian menggunakan pendekatan kualitatif dengan studi dokumentasi email yang terkait dengan BEC dan wawancara kepada sejumlah sumber primer yang terlibat dalam penanganan kasus BEC. Hasil analisis menunjukkan perkembangan komunikasi dalam BEC yang melalui fase komunikasi impersonal, interpersonal, dan hiperpersonal. Hasil analisis juga menunjukkan adanya upaya persuasi dari pelaku BEC dengan mengarahkan korban pada rute periferal dengan satu atau sedikit isyarat agar terjadi perubahan sikap dalam bentuk bersedia mentransfer sejumlah dana kepada rekening yang disediakan oleh pelaku. Bila rute periferal tidak cukup meyakinkan korban, pelaku BEC akan menggunakan rute sentral dengan membangun persuasi dari aspek motivasi, kemampuan, dan argumentasi yang kuat.

Kata Kunci: *business email compromise, computer-mediated communication, persuasi*

Abstract

Business Email Compromise (BEC) has become a new mode of cyber crime in the form of phishing emails to targeted individuals or corporations for financial benefits. This article discusses the concept of BEC in the scope of mediated communication and persuasion from the perpetrator to the victim and is related to the theory of Computer-Mediated Communication and the Elaboration Likelihood Model. The research method uses a qualitative approach with a study of email documentation related to BEC and interviews with a number of primary sources involved in handling BEC cases. The results of the analysis show the development of communication in BEC which goes through the phases of impersonal, interpersonal, and hyperpersonal communication. The results of the analysis also show that there was an attempt at persuasion from the BEC perpetrators by directing the victim on a peripheral route with one or a few cues so that there would be a change in attitude in the form of being willing to transfer a certain amount of funds to the account provided by the perpetrator. If the peripheral route is not enough to convince the victim, the BEC perpetrator will use the central route by building persuasion from aspects of motivation, ability, and strong arguments.

Keywords: business email compromise; computer-mediated communication; persuasion

PENDAHULUAN

Perkembangan teknologi yang semakin canggih berefek pada aspek sosial dan ekonomi dari bentuk yang tradisional menjadi modern (Muzaini, 2014). Kemudahan dalam proses pembuatan, penyimpanan, pemrosesan, pentransmisian, hingga pengambilan informasi berkontribusi pada peningkatan kuantitas data, meningkatkan komunikasi virtual, mengembangkan jaringan sosial, namun di sisi lain, meningkatkan risiko, ancaman, dan bahaya yang tidak dapat diabaikan (Li, 2015). Sebagian besar kejahatan dunia maya yang kita lihat hari ini hanya mewakili migrasi kejahatan dunia nyata ke dunia maya. Ruang siber menjadi alat yang digunakan penjahat untuk melakukan kejahatan lama dengan cara baru (Brenner, 2010). Ruang siber dianggap sebagai lingkungan yang aman bagi penjahat untuk menjalankan tindak kriminal dengan memanfaatkan celah keamanan jaringan karena penegakan hukum yang tidak efisien (Shahbazi, 2019).

Istilah kejahatan siber dicetuskan oleh Sussman dan Heuston pada tahun 1905. Istilah ini tidak dapat dicakup hanya dalam satu definisi tertentu, tetapi lebih dilihat sebagai kumpulan tindakan atau pelanggaran berdasarkan modus operandi yang mempengaruhi data di sistem komputer (Sabillon et al., 2016). Pada prinsipnya, kejahatan siber merupakan tindakan ilegal di mana perangkat digital atau sistem informasi merupakan alat atau target, atau merupakan kombinasi keduanya. Istilah kejahatan siber (*cybercrime*) beririsan dengan istilah lain seperti kejahatan komputer (*computer crime*), kejahatan elektronik (*electronic crime*), *e-crime*, kejahatan teknologi tinggi (*high-technology crime*), kejahatan era informasi (*information age crime*), kejahatan sibernetik (*cybernetic crime*), kejahatan terkait komputer (*computer-related crime*), hingga kejahatan digital (*digital crime*). Kejahatan siber bersifat kompleks, dan dapat ditelaah dari ragam perspektif seperti ekonomi, ideologi, hasrat, bahkan dendam tertentu (Leukfeldt et al., 2017).

Awal mula kejahatan siber menggunakan komputer dimulai sejak akhir 1940-an hingga akhir 1960-an, ketika masyarakat umum masih memandang komputer sebagai instrumen yang "kadang tidak dapat diandalkan" tetapi "cenderung aman". Perkembangannya berlanjut ketika di tahun 1950-an kejahatan siber menggunakan komputer merambah di bidang militer, teknik, sains, keuangan, dan perdagangan. Dokumentasi paling awal terkait penyalahgunaan komputer yang melibatkan perbankan terjadi pada tahun 1958, dan proses penuntutannya membutuhkan jangka waktu hingga delapan tahun pada tahun 1966 (Li, 2017). Taksonomi kejahatan siber di bidang keuangan berdasarkan sifat alamiahnya terdiri atas penipuan terkait identitas diri, spionase, eksploitasi infrastruktur keuangan yang sudah ada, serangan-serangan yang mengganggu, kejahatan terkait konten, serta penipuan online dan pembajakan (Lagazio et al., 2014).

Kejahatan siber merambah dalam berbagai jenis. Secara umum kejahatan tersebut terdiri atas (Pitts, 2017): (1) Peretasan (*hacking*), jenis kejahatan di mana komputer seseorang dibobol sehingga informasi pribadi atau sensitif dapat dikuasai. Dalam peretasan, pelaku menggunakan berbagai perangkat lunak untuk memasuki komputer seseorang yang tidak menyadari bahwa komputernya sedang diakses dari suatu lokasi; (2) Pencurian (*theft*), jenis kejahatan ketika seseorang melanggar hak cipta dalam bentuk seperti mengunduh musik, film, game, dan perangkat lunak secara ilegal; (3) *Cyber stalking*, jenis pelecehan secara *online* dimana korban menjadi sasaran rentetan pesan online ataupun email.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Dalam jenis ini, pelaku biasanya mengenal korban namun memilih menguntitnya secara *online*; (4) Pencurian identitas (*identity theft*), kejahatan dalam bentuk akses data ke rekening bank, kartu kredit, jaminan sosial, dan informasi privat lainnya guna menyedot uang atau membeli barang secara online atas nama korban. Kejahatan jenis ini mengakibatkan kerugian finansial yang besar dan bahkan merusak riwayat kredit korban; (5) Perangkat lunak berbahaya (*malicious software*), perangkat lunak atau program berbasis internet yang digunakan untuk mengganggu jaringan dan mendapatkan akses ke sistem dan mencuri informasi atau data sensitif yang menyebabkan kerusakan pada perangkat lunak di dalam sistem; dan (6) *Child soliciting and abuse*, jenis kejahatan dalam bentuk membawa anak di bawah umur masuk ke dalam suatu *chat rooms* untuk keperluan pornografi anak.

Dalam konteks Indonesia, kejahatan siber menjadi persoalan yang makin mengkhawatirkan. Wakil Kepala Kepolisian RI Komisaris Jenderal Polisi Syafruddin pada tahun 2018 mengungkapkan bahwa Indonesia berada pada posisi kedua kejahatan siber di dunia (Kominfo.go.id, 2018). Dalam Diskusi Kontemporer yang diselenggarakan oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) bersama dengan Universitas Padjadjaran pada 1 Desember 2020, Wakil Direktur Tindak Pidana Siber Badan Reserse Kriminal Polri Komisaris Besar Polisi Himawan Bayu Aji menyebut tren kejahatan yang ditangani oleh Direktorat Tindak Pidana Siber Bareskrim Polri terus meningkat seperti ditunjukkan oleh grafik 1.

Grafik 1 Tren Kejahatan Siber

Sumber: Direktorat Tindak Pidana Siber Bareskrim Polri, 2020

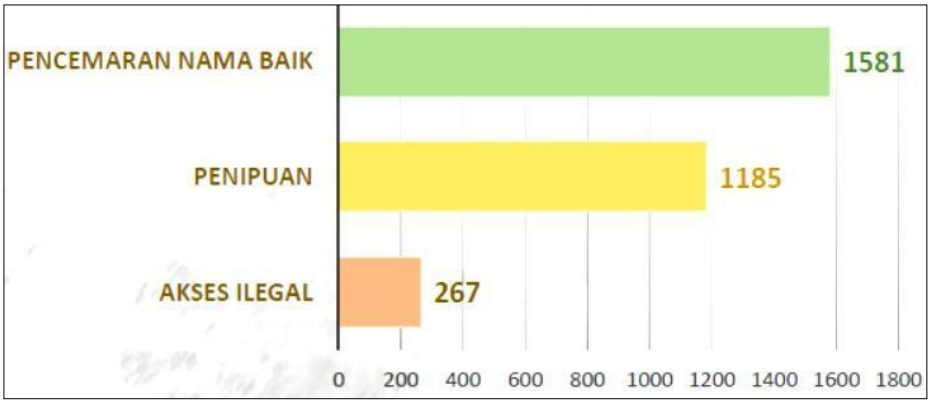
Keterangan:
CT: *Cyber Threat*
CC: *Cyber Crime*

Di masa pandemi Covid-19, kejahatan siber justru mengalami peningkatan. Secara global, pandemi Covid-19 menghasilkan sejumlah siber dalam bentuk *phishing*, *malware*,

Jurnal Riset Komunikasi JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

financial fraud, pharming, hacking, extortion, dan *denial of service* hanya dalam periode Desember 2019 hingga Maret 2020 (Lallie et al., 2021). Sementara di Indonesia, selama periode Februari hinga April 2020, sejumlah serangan siber dilakukan dalam bentuk *malware, DDoS, zoombombing,* dan *fraud* seperti dalam bentuk pencurian informasi perbankan, penggunaan gambar-gambar yang mengganggu, sabotase, penipuan donasi untuk kepentingan oknum tertentu, dan berbagai bentuk lainnya. Serangan tersebut menargetkan masyarakat umum dan lembaga keuangan pada khususnya (Amarullah et al., 2021). Meningkatnya kecemasan yang disebabkan oleh pandemi meningkatkan potensi keberhasilan serangan siber sesuai dengan peningkatan jumlah dan jangkauan serangan siber tersebut. Data Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian RI selama periode Januari hingga November tahun 2020 menemukan kasus penipuan dan akses ilegal menjadi bagian dari tiga tren kejahatan tertinggi selama masa pandemi. Rinciannya terdiri atas 1581 kasus pencemaran nama baik, 1185 kasus penipuan, dan 267 akses ilegal yang dijelaskan di grafik 2 (Direktorat Tindak Pidana Siber Bareskrim Polri, 2020).

Grafik 2 Tren Kejahatan Siber selama Pandemi Covid-19
Periode Januari – November 2020



Sumber: Direktorat Tindak Pidana Siber Bareskrim Polri, 2020

Dari keseluruhan bentuk kejahatan siber, muncul salah satu modus yang dikenal dengan *business email compromise* (BEC), yang dikenal juga dengan "*CEO fraud*" atau "*man-in-the middle scam*" (Saud Al-Musib et al., 2021). BEC menjadi bentuk kejahatan yang riil ketika penjahat di dunia maya dapat mengeksploitasi jaringan email untuk melakukan serangan siber terhadap suatu korporasi demi keuntungan finansial, dikarenakan email telah menjadi mode komunikasi yang umum di seluruh dunia. Dilansir dari data PPATK, BEC telah menjadi persoalan global dalam kurun waktu lima tahun terakhir dengan kerugian yang diderita para pelaku bisnis mencapai puluhan miliar dolar Amerika Serikat setiap tahunnya. Di tahun 2020 kejahatan siber dalam bentuk BEC mengalami peningkatan signifikan hingga lebih dari 200 persen (Grafik 3).

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Grafik 3 Peningkatan BEC selama Tiga Kuartal Pertama Tahun 2020

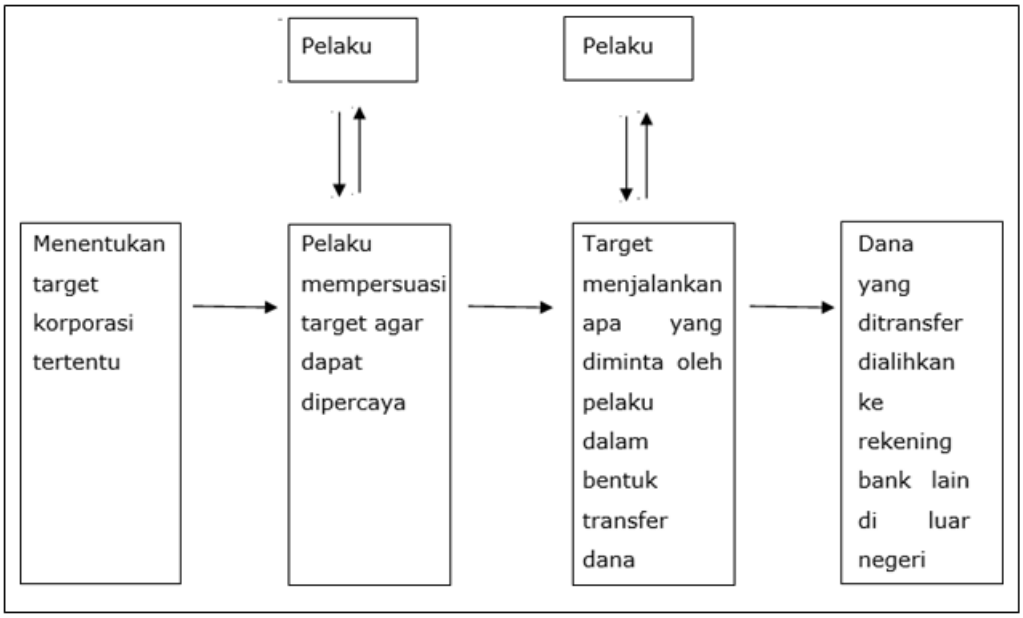
Sumber: Al-Musib et al., 2021

Dalam konteks Indonesia, BEC tercatat sudah terjadi dalam dua tahun terakhir dan kecenderungannya semakin meningkat akibat pandemi. Pelaku kejahatan dalam bentuk BEC memanfaatkan suasana kecemasan dan ketidakpastian yang ditimbulkan oleh krisis yang terjadi akibat pandemi Covid-19. Data PPATK mencatat selama periode Juli 2020 hingga Juli 2021, hasil kejahatan yang masuk ke dalam sistem perbankan nasional mencapai angka Rp 300 miliar, dengan nominal Rp 175 miliar berhasil diselamatkan. Sisa dari nominal tersebut tidak berhasil diselamatkan karena sudah ditarik oleh pelaku, yang hingga kini masih dalam proses penyidikan oleh Kepolisian (Antaranews.com, 2021). Biro Investigasi Federal (FBI) secara umum menjelaskan empat tahapan terjadinya BEC (fbi.gov, 2017).

Tahap pertama adalah identifikasi target, dengan memanfaatkan informasi yang tersedia secara *online* untuk mengenal profil perusahaan yang ditargetkan berikut eksekutifnya. Tahap kedua adalah *phishing email* sekaligus membangun kepercayaan, dalam bentuk pengiriman *email* yang sudah diretas dengan menargetkan pejabat di perusahaan yang biasanya berposisi di divisi keuangan. Pelaku BEC menggunakan teknik persuasi dan tekanan untuk memanipulasi dan mengeksploitasi sifat alamiah manusia. Tahapan ini dapat terjadi selama beberapa hari atau beberapa minggu. Tahapan ketiga merupakan tahap pertukaran informasi. Korban berhasil diyakinkan bahwa ia sedang melakukan transaksi bisnis yang sah. Korban kemudian mulai menyiapkan mekanisme transfer atau pembayaran kepada pelaku. Tahapan terakhir adalah transfer rekening ke tujuan yang sudah dimanipulasi dalam email. Setelah transfer dilakukan, dana akan diarahkan ke rekening bank yang dikendalikan oleh kelompok kejahatan terorganisir. Di tahap ini, pelaku bahkan masih dapat terus mempersuasi korban untuk mentransfer lebih banyak dana (fbi.gov, 2017) seperti ditunjukan oleh gambar 1.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 1 Tahapan *Business Email Compromise*



Sumber: (Saud Al-Musib et al., 2021)

Karena modus penipuan BEC tergolong baru muncul dan berkembang, berbagai penelitian terkait topik tersebut relatif baru mulai bermunculan sejak tahun 2016 hingga saat ini. Penelitian yang sudah dibuat hingga kini lebih banyak mengambil perspektif di bidang audit forensik maupun teknologi informasi. Sebagai contoh, dalam "*Business Email Compromise (BEC) Attacks*" oleh Norah Saud Al-Musib, Faeiz Mohammad Al- Serhani, Mamoona Humayun, dan N.Z. Jhanjhi, dijelaskan mengenai analisis BEC, bagaimana BEC dapat terjadi, cara menghindari atau meminimalisir kejadiannya, dan dampaknya terhadap organisasi. Kesimpulan dari penelitian ini antara lain prediksi penyebaran dan perkembangan BEC di masa depan karena ketergantungan korporasi pada teknologi yang begitu tinggi (Saud Al-Musib et al., 2021).

David Zweighaft dalam *"Business email compromise and executive impersonation: are financial institutions exposed?"* yang dimuat di *Journal of Investment Compliance* pada 2017 menjelaskan makin populernya modus penipuan dalam bentuk BEC dan ancaman yang ditimbulkannya spesifik terhadap lembaga keuangan. Zweighaft menyimpulkan bahwa lembaga keuangan harus memahami potensi risiko hukum dan regulasi yang ditimbulkan akibat BEC dan peniruan identitas eksekutif korporasi (*executive impersonation*), sekaligus perlunya menciptakan budaya skeptis, proaktif, dan kesadaran yang tinggi guna memerangi penipuan dalam bentuk BEC (Zweighaft, 2017).

Dalam IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C) tahun 2020, Songpon Teerakanok, Hiroaki Yasuki, dan Tetsutaro Uehara menulis *"A Practical Solution Against Business Email Compromise (BEC) Attack using Invoice Checksum"*. Tulisan tersebut mencoba memberikan solusi praktis mengatasi BEC menggunakan *invoice checksum*, yang dapat digunakan melalui aplikasi di *smartphone* (Teerakanok et al., 2020).

Penelitian yang berfokus pada aspek komunikasi dilakukan oleh Christiany Juditha, dengan judul "Pola Komunikasi dalam *Cybercrime* (Kasus *Love Scams*)" pada tahun 2015 yang menggunakan teori *Computer Mediated Communication* (C. Juditha, 2015). Namun, kasus yang diangkat sama sekali tidak terkait dengan BEC, seiring BEC yang mulai muncul pada sekitar tahun 2016 dan terus berkembang hingga kini.

Email sebagai sarana BEC menjadi kunci dari penelitian ini. Email merupakan bagian dari teknologi komunikasi baru yang dapat dijelaskan dengan teori *Computer-Mediated Communication* (CMC). Secara umum, CMC membahas bagaimana antarmanusia dapat saling berkomunikasi dengan menggunakan perangkat berbasis komputer (Setiawan et al., 2020). Smith menyebutkan empat aspek interaksi virtual yang membentuk perilaku komunikasi dalam CMC, meliputi interaksi virtual yang bersifat spasial atau tidak mengenal ruang dan jarak; bersifat asinkron atau tidak beriringan; bersifat *acorporeal* atau tidak jasmaniah; dan bersifat *astigmatic* atau meniadakan diferensiasi sosial berdasarkan stigma sosial (Juditha, 2018). CMC seperti dalam bentuk email merupakan cara pencarian informasi yang murah untuk meningkatkan efisiensi dan produktivitas (Ean, 2011). Efisiensi yang ditimbulkan dari komunikasi melalui email menjadikan penipuan dalam bentuk BEC menjadi relevan untuk dilakukan.

Joseph Walter membagi perspektif CMC ke dalam tiga fase, yaitu interaksi impersonal, interaksi interpersonal, dan interaksi hiperpersonal (Walther, 1996). Di interaksi impersonal, CMC dapat diartikan sebagai perilaku komunikasi antara individu dengan komputer yang bersifat *task-oriented* atau berorientasi kerja. Dalam interaksi impersonal, diharapkan suatu tugas atau pekerjaan dapat dilaksanakan lebih efektif dibandingkan pertemuan tatap muka (*face-to-face*), seperti dalam bentuk email. Tahapan BEC selalu diawali dengan persoalan yang bersifat impersonal, karena memang tujuannya berupa keuntungan ekonomi dengan modus penipuan dari suatu korporasi yang ditargetkan dengan menggunakan sarana email. Seiring proses komunikasi terus berlanjut, percakapan antara pelaku dengan targetnya melalui perantara email beranjak ke fase berikutnya yaitu interaksi interpersonal.

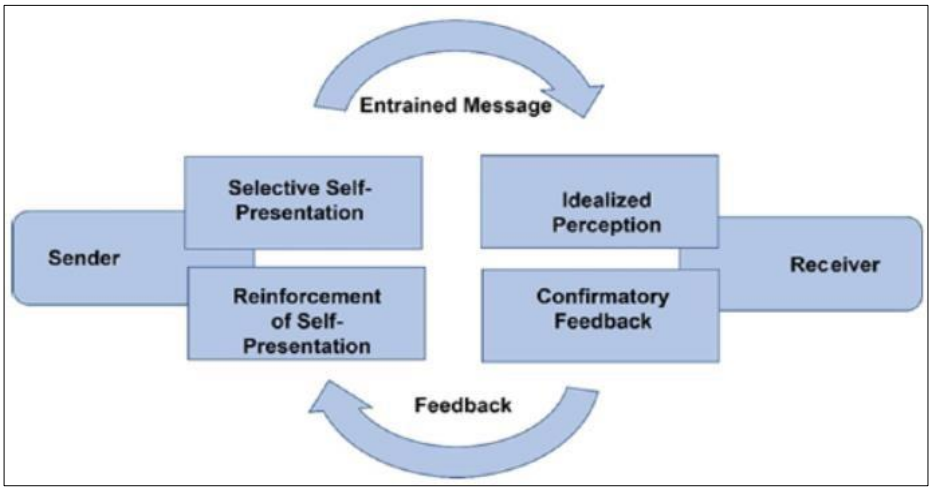
Modus penipuan dalam bentuk BEC juga dapat dijelaskan dalam model interaksi hiperpersonal seperti dijelaskan dalam Gambar 2. Dari faktor pengirim atau pelaku kejahatan BEC, ia akan melakukan optimal *self-presentation* yang dirancang untuk menonjolkan hal tertentu dan menyembunyikan hal lainnya demi mengelola citra virtualnya. Hal ini disalurkan melalui *channel entrainment*, yang mengacu pada kemampuan pengirim untuk menyinkronkan pesan dengan presentasi diri yang difasilitasi oleh saluran komunikasi tertentu dan terkait erat dengan sinkronisitas dan kekayaan saluran. Semakin cepat informasi dan umpan balik dipertukarkan, serta semakin banyak isyarat yang dapat dipertukarkan secara bersamaan, semakin sedikit kesempatan bagi individu untuk secara hati- hati membangun pesan mereka untuk mencapai tujuan relasional strategis yang terkait dengan waktu dan tempat pesan itu disampaikan kepada penerima (Carr, 2021).

Dalam interaksi hiperpersonal, penerima (*receiver*) akan membangun persepsi ideal terhadap pengirim pesan. Hal ini terjadi karena tidak adanya isyarat tatap muka dan pengetahuan memadai terhadap pengirim pesan, sehingga tercipta porsi persepsi yang sangat besar yang disebut *overattribution*. Setelah proses komunikasi terbangun dari pemberi pesan

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

kepada penerima pesan melalui medium tertentu, terdapat umpan balik (*feedback*) yang disebut *behavioral communication* atau konfirmasi perilaku. Hal ini merupakan proses di mana antar pasangan yang berkomunikasi membangun kesan, citra, dan intimasi dari lawan bicaranya saat komunikasi terjadi (Walther, 1996).

Gambar 2 Faktor dan Hubungan Pembentuk Model Hiperpersonal



Sumber: Walther, 1996

Setelah proses pengambilalihan email selesai dilakukan, tahap lanjutan dari BEC adalah pengiriman email kepada target dari korporasi yang dituju. Pada umumnya, email dikirimkan kepada personel di bagian keuangan korporasi tersebut. Email penipuan dengan modus BEC lazimnya menonjolkan otoritas dari pengirim email sekaligus menunjukkan urgensi perlunya transfer dana segera dilakukan. Namun tidak sedikit email dari pelaku kejahatan berupa persuasi kepada korban tujuannya, terutama bila email dilakukan dalam konteks sebagai mitra bisnis, bukan atasan dan bawahan dalam suatu korporasi.

Persuasi dalam penipuan bermodus BEC dapat diuraikan menggunakan teori persuasi terkemuka, yaitu Model Kemungkinan Elaborasi. Premis teori ini adalah bahwa manusia terkadang mengevaluasi pesan dengan cara yang rumit, menggunakan pemikiran kritis, dan terkadang juga dilakukan dengan cara yang lebih sederhana dan tidak terlalu kritis (Littlejohn et al., 2017). Persuasi merupakan suatu peristiwa kognitif. Target pesan persuasif akan menggunakan proses mental berupa motivasi dan pemahaman guna mencerna pesan tersebut. Pesan yang diterima akan ditujukan di antara dua rute yang dapat dipilih pada salah satunya, atau merupakan kombinasi dari dua rute tersebut, yang dikenal dengan rute sentral dan rute periferal.

Dalam rute sentral, pesan dirutekan secara terpusat (*central route/elaborated route*). Jalur pemrosesan kognitif dalam rute sentral melibatkan pemeriksaan/elaborasi isi pesan, sejauh mana seseorang dengan hati-hati memikirkan argumen yang relevan dengan masalah yang terkandung dalam komunikasi persuasif. Dalam hal ini, elaborasi membutuhkan upaya kognitif tingkat tinggi. Upaya tersebut meliputi kehati-hatian dalam meneliti suatu gagasan, mencari tahu manfaat dari gagasan tersebut, hingga merenungkan implikasinya. Gagasan

yang masuk ke dalam rute sentral akan melalui tahapan motivasi, kemampuan (*ability*), dan penilaian akan argumentasi persuasi yang disampaikan (Griffin et al., 2018).

Pemrosesan kognitif dalam rute sentral bersifat kompleks, mencakup banyak informasi, pelibatan argumen rasional, serta pembuktian untuk mendukung kesimpulan tertentu. Pelaku BEC akan menggunakan motivasi yang meyakinkan korbannya dalam bentuk narasi di email, disertai dengan ekspresi yang seolah mengungkapkan keahlian si pelaku dalam bidang pekerjaan tertentu. Yang paling utama, pelaku BEC akan membangun argumentasi yang kuat kepada korbannya walaupun dimediasi dengan menggunakan instrumen berupa email.

Di sisi lain, rute periferal merupakan proses jalan pintas bagi mental yang menerima atau menolak pesan berdasarkan sejumlah isyarat. Proses menggunakan isyarat dalam rute periferal merupakan lawan dari berpikir aktif tentang suatu pesan yang termasuk berada dalam rute sentral. Pada faktanya, penerima pesan tidak akan setiap waktu berada dalam keadaan termotivasi atau mampu untuk memahami suatu pesan yang sama setiap harinya. Karena itulah, pengalihan rute dari rute sentral ke rute periferal menjadi hal yang sangat mungkin terjadi (Dainton & Zelley, 2019). Asumsi dalam CMC dan proses persuasi yang terjadi dalam BEC membentuk pola komunikasi tersendiri. Pola komunikasi diartikan sebagai bentuk atau pola hubungan antara dua orang atau lebih dalam proses pengiriman dan penerimaan cara yang tepat sehingga pesan yang dimaksud dapat dipahami (Juditha, 2018).

Penelitian ini menjadi penelitian pertama yang menganalisis pola komunikasi persuasi dalam penipuan dengan modus BEC yang diprediksi masih akan menjadi ancaman riil dalam beberapa tahun mendatang. Seperti telah dijelaskan, BEC menjadi salah satu kejahatan siber paling berbahaya saat ini dengan kerugian masif yang ditimbulkannya. Penelitian ini berfokus pada proses manipulasi dan persuasi yang dilakukan pelaku kepada targetnya dengan menganalisis pola komunikasi dalam BEC. Hal ini menarik untuk diteliti mengingat proses BEC sepenuhnya terjadi melalui saluran email tanpa pertemuan tatap muka, namun tetap berhasil mempengaruhi korban karena manipulasi dan persuasi yang dilakukan oleh pelaku. Tujuan penelitian adalah mendeskripsikan pola komunikasi yang dilakukan pelaku kepada korban dalam penipuan dengan modus BEC.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Pendekatan kualitatif adalah suatu proses penelitian dan pemahaman yang berdasarkan pada metodologi yang menyangkut suatu fenomena sosial dan masalah-masalah manusia. Melalui pendekatan ini, peneliti membuat suatu gambaran kompleks, meneliti kata-kata, menyusun laporan terperinci dari pandangan responden, dan melakukan studi pada situasi yang dialami (Creswell, 1998). Metode ini digunakan karena mampu menjelaskan hubungan antarkategori yang ditemukan dan disusun dalam penelitian ini. Metode kualitatif juga dapat menggambarkan sekaligus menganalisis pola perilaku manusia (Hidayat, 2017). Dalam hal ini, pendekatan kualitatif menjadi pendekatan yang relevan untuk mengalisisi pola komunikasi dan persuasi dalam penipuan berbentuk BEC, karena penelitian bertujuan untuk

mendalami suatu peristiwa hingga menganalisis pola perilaku dalam bentuk komunikasi persuasi dalam kasus BEC.

Metode dalam penelitian ini menggunakan studi kasus, yang menjadi strategi yang cocok bila pokok pertanyaan suatu penelitian berkenaan dengan jawaban atas bagaimana dan mengapa. Dalam studi kasus, peneliti dapat mengontrol peristiwa-peristiwa yang akan diteliti dan fokus penelitian berpusat pada fenomena di masa kini (Yin, 2009). Beberapa karakteristik dari studi kasus, yaitu (1) mengidentifikasi "kasus" untuk suatu studi; (2) kasus tersebut merupakan sebuah "sistem yang terikat" oleh waktu dan tempat; (3) menggunakan berbagai sumber informasi dalam pengumpulan datanya untuk memberikan gambaran secara terperinci dan mendalam tentang respons dari suatu peristiwa; dan (4) pendekatan studi kasus akan "menghabiskan waktu" dalam menggambarkan konteks atau setting untuk suatu kasus (Creswell, 1998). Pendekatan studi kasus diterapkan guna mendapat pemahaman terkait suatu masalah, peristiwa, atau fenomena yang menarik dalam konteks kehidupan nyata yang alami (Nurahma & Hendriani, 2021).

Metode studi kasus akan menjelaskan proses BEC secara terperinci dan mendalam guna memperoleh pemahaman memadai tentang kasus ini. Terdapat enam bentuk pengumpulan data dalam studi kasus, yang meliputi (1) dokumentasi yang terdiri dari surat, memorandum, agenda, laporan-laporan suatu peristiwa, proposal, hasil penelitian, hasil evaluasi, kliping, dan artikel; (2) rekaman arsip yang terdiri dari rekaman layanan, peta, data survei, daftar nama, rekaman- rekaman pribadi seperti buku harian, kalender, dan sebagainya; (3) wawancara yang biasanya bertipe *open- ended*; (4) observasi langsung; (5) observasi partisipan; dan (6) perangkat fisik atau kultural yaitu peralatan teknologi, alat atau instrumen, pekerjaan seni, dan lain-lain (Kusmarni, 2012).

Dalam penelitian ini, data yang digunakan berupa studi dokumentasi dan wawancara mendalam dari berbagai sumber dan pihak-pihak terkait. Pengumpulan data berupa email dalam modus BEC dilakukan dengan studi dokumentasi dari berbagai sumber yang bersifat terbuka dan terpercaya, seperti melalui situs Biro Investigasi Federal Amerika Serikat (FBI). Dokumentasi email yang terkumpul merupakan contoh dari modus BEC dengan perubahan nama individu maupun korporasi, mengingat korespondensi email antara pelaku BEC dengan targetnya diklasifikasikan sebagai informasi yang bersifat rahasia dalam konteks penegakan hukum.

Pendalaman informasi dilakukan dengan proses wawancara kepada sejumlah informan dengan kriteria (1) memiliki pemahaman yang memadai terkait proses BEC dan (2) secara spesifik memiliki profesi yang terkait dengan proses penanganan BEC. Pemilihan informan dilakukan dengan teknik *purposive sampling*. Informan terdiri atas tiga orang yang bekerja di Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dengan masing-masing informan secara spesifik memiliki peran sebagai penanggungjawab penanganan kasus BEC, penegak hukum yang menangani persoalan BEC melalui skema *Public-Private Partnership* (PPP), dan seorang pranata kehumasan yang bertugas menyiapkan keterangan pers dan publikasi mengenai peran serta PPATK dalam menanganai perkara BEC. Seorang informan lagi merupakan personel Biro Investigasi Federal (FBI) Amerika Serikat yang bertugas di Kedutaan Besar Amerika Serikat di Jakarta.

Tabel 1 Data Informan

No.	Informan	Pekerjaan
1	Savetri Lihanara	Koordinator Analis Transaksi Keuangan Bank PPATK
2	Rista Sihombing	Analis Kerja Sama PPATK
3	Dhiyah Ferawaty	Pranata Humas PPATK
4	BG	Penyidik FBI

Sumber: Olahan Peneliti, 2022

Analisis data pada penelitian ini bersifat induktif, yaitu suatu analisis berdasarkan data yang diperoleh. Setelahnya dikembangkan pola hubungan tertentu hingga disimpulkan menjadi data yang valid dan mudah dipahami. Peneliti menggunakan analisis data dengan model Miles dan Huberman, yaitu pengumpulan data yang dilakukan secara berulang hingga tuntas dan didapati data yang dianggap kredibel (Sugiyono, 2009). Langkah-langkah proses analisis data dalam penelitian ini meliputi (a) reduksi data, dalam bentuk merangkum, memilih hal-hal yang pokok, memfokuskan hal-hal yang penting, dicari tema dan polanya dan membuang yang tidak perlu; (b) penyajian data, yaitu merangkai data yang memudahkan untuk membuat kesimpulan/tindakan yang diusulkan. Tujuannya adalah menyederhanakan informasi yang bersifat kompleks menjadi informasi yang sederhana hingga mudah dipahami maksudnya; dan (c) penarikan kesimpulan, dengan mencermati dan menggunakan pola pikir yang dikembangkan. Penarikan kesimpulan menjawab semua rumusan masalah yang telah ditetapkan oleh peneliti dalam penelitian ini. Penelitian ini juga menggunakan analisis deskriptif, yang digunakan untuk mendeskripsikan dan menginterpretasikan hasil penelitian tentang bagaimana model komunikasi dan persuasi dijalankan dalam skema penipuan dengan modus BEC.

HASIL DAN PEMBAHASAN

Modus BEC terjadi karena faktanya begitu banyak individu maupun pelaku bisnis menjalankan bisnisnya dengan mengandalkan email (Cross & Gillett, 2020). Pelaku BEC memanfaatkan hal ini dengan mengirim pesan email yang tampaknya berasal dari sumber yang diketahui membuat permintaan yang sah dengan berbagai triknya, termasuk dengan menggunakan pendekatan persuasi. Rilis PPATK pada 18 Agustus 2021 menyebutkan hasil kejahatan yang masuk ke dalam sistem perbankan Indonesia telah mencapai angka Rp 300 miliar, dan hanya Rp 175 miliar yang berhasil diselamatkan. Praktik BEC yang biasanya bersifat transnasional juga mempersulit upaya investigasi yang dilakukan oleh aparat penegak hukum.

Terdapat tiga faktor yang membuat partner komunikasi via komputer cenderung lebih menarik, yaitu (1) email dan jenis komunikasi lainnya memungkinkan presentasi diri yang sangat selektif, dengan lebih sedikit penampilan atau perilaku yang tidak diinginkan dibandingkan komunikasi langsung. Dengan kata lain, individu tidak perlu repot menata perilaku visual ketika berkomunikasi melalui internet; (2) orang yang terlibat dalam komunikasi via komputer terkadang mengalami atribusi yang berlebihan dalam membangun

kesan stereotip tentang partner komunikasinya. Kesan-kesan seperti ini cenderung mengabaikan informasi negatif seperti kesalahan cetak, kesalahan ketik, dan bentuk kesalahan lainnya; dan (3) ikatan intensifikasi bisa terjadi di mana pesan-pesan positif dari seorang partner komunikasi akan membangkitkan pesan-pesan positif (Juditha, 2015).

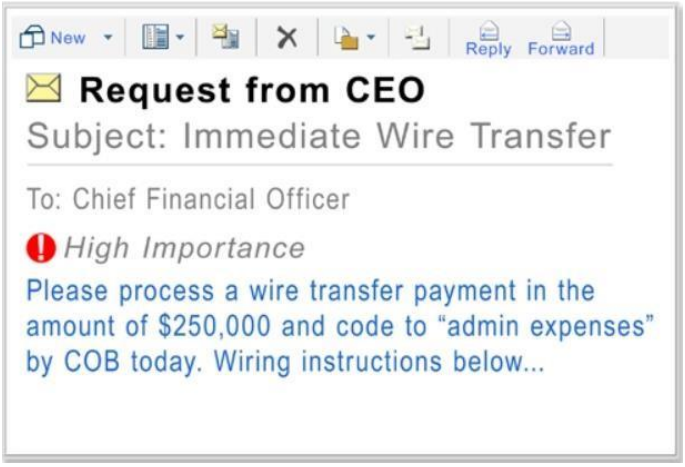
BEC sebagai interaksi impersonal-interpersonal-hiperpersonal

Dalam wawancara dengan informan dari FBI, BG, ia menyampaikan makin canggihnya pola *hacking, phishing*, hingga *malware* dari pelaku kejahatan siber, termasuk dengan modus BEC. Kejahatan ini tidak dilakukan seorang diri dan tergolong dalam kejahatan yang sangat terorganisir. Modifikasi bentuk dan pola kejahatan terus dilakukan, dengan penetapan target yang juga bersifat dinamis. Pelaku kejahatan siber juga semakin meluas dan terbukti dapat dilakukan oleh siapa saja. Ia menyebutkan kasus di Jawa Timur pada April 2021 saat Kepolisian Daerah Jawa Timur menangkap pembuat dan penyebar *website* palsu atau *scampage*. Para tersangka melakukan aksinya sejak Mei 2020 hingga Maret 2021 dengan menyebarkan domain palsu ke 27 juta nomor telepon warga Amerika Serikat. Sekitar 30 orang tertipu dan menjadi korban dari 14 negara bagian di AS dengan keuntungan yang diperoleh para tersangka sekitar 30.000 dolar AS atau setara dengan Rp 420 juta (Detik.com, 2021). BG menyebut bahwa kasus ini bahkan baru diketahui FBI setelah Polda Jawa Timur bergerak cepat dan menjalankan koordinasi. Kasus ini juga menjadi contoh bahwa perkara kejahatan siber menjadi semakin serius seiring perkembangan teknologi informasi yang kini mudah diakses siapa saja. Sementara itu, Analis Kerja Sama Internasional Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), Rista Sihombing, menyampaikan bahwa kerja PPATK dalam menanggulangi BEC melibatkan jejaring organisasi kejahatan yang berada di Italia, Belanda, Amerika Serikat, Jerman, Turki, Jepang, dan beberapa negara lainnya tanpa harus melalui proses tatap muka.

Fase impersonal dalam praktik BEC terjadi sejak awal kemunculannya sekitar tahun 2016, dengan mayoritas bentuknya berupa email yang terkait dengan permintaan transfer dana terkait proyek pekerjaan tertentu. Seperti dalam Gambar 3, salah satu contoh email dalam BEC menunjukkan adanya instruksi dari seorang Chief Executive Officer (CEO) yang telah mengalami *email phishing* kepada Chief Financial Officer (CFO) perusahaan yang sama untuk memproses pembayaran sejumlah 250.000 dolar AS dengan urgensi untuk dilaksanakan segera pada hari yang sama, dan petunjuk transfer yang disampaikan melalui email tersebut.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 3 BEC di Fase Impersonal

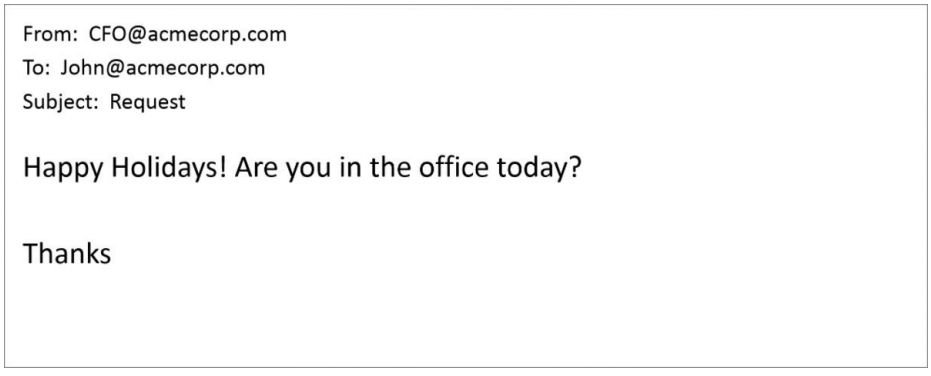


Sumber: FBI, 2017

Pada perkembangannya, BEC tidak berhenti pada fase impersonal. Layaknya perkembangan fase dalam *Computer- Mediated Communication*, modus BEC melangkah ke fase interpersonal karena terbangunnya suatu hubungan sosial via email. Sistem komunikasi yang dimediasi komputer dalam berbagai bentuk, telah menjadi bagian integral dari inisiasi, pengembangan, dan pemeliharaan hubungan interpersonal. Dalam hal ini, terjadi pembentukan komunikasi yang halus di hampir setiap konteks relasional (Walther, 2011).

Dalam fase interpersonal, pertukaran informasi yang terjadi antara pelaku dan korban mengalami peningkatan seiring meningkatnya waktu berkomunikasi. Pelaku sebagai komunikator berfokus pada upaya mencari informasi tentang korban guna mendapat informasi selengkap mungkin. Seperti ditunjukkan dalam Gambar 4, pelaku tidak serta-merta merujuk pada suatu pekerjaan yang harus dilaksanakan, namun dimulai dengan sapaan hangat seperti "Selamat berlibur" atau upaya lain untuk mencari tahu apa yang sedang dilakukan korban pada saat email dikirimkan oleh pelaku.

Gambar 4 BEC di Fase Interpersonal



Sumber: FBI, 2017

Fase hiperpersonal dalam proses BEC terjadi ketika walaupun pelaku dan korban terpisah jarak secara fisik dan berkomunikasi melalui email dengan isyarat terbatas, pelaku dapat membangun presentasi diri dan mengubah gaya komunikasinya. Hal ini menyebabkan

terjadinya idealisasi dari pelaku sebagai pengirim pesan dan disempurnakan dengan komunikasi yang bersifat asinkronis. Dengan demikian, pelaku sebagai pengirim pesan dan korban sebagai penerima pesan memiliki waktu yang cukup untuk mempertimbangkan pesan yang terkirim dan yang diterima (Walther, 1996).

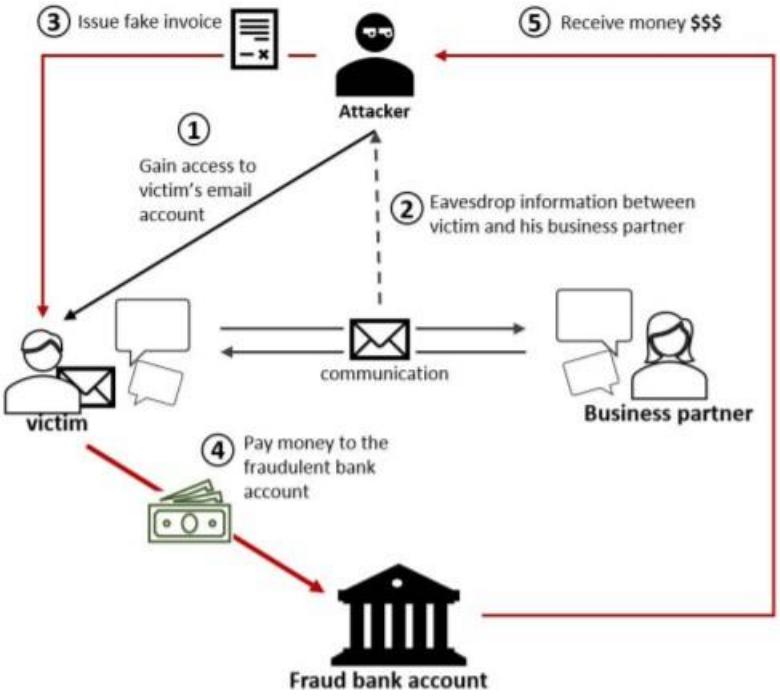
Proses terjalinnya komunikasi hiperpersonal dalam kasus BEC berproses dalam model yang meliputi pengirim pesan, penerima pesan, saluran, dan umpan balik (*feedback*). Dari sisi pelaku yang mengirimkan pesannya, dilakukan proses presentasi diri yang selektif guna mengelola citra virtual yang berkesan dengan baik. Pelaku sangat mungkin melakukan manipulasi pesan dalam komunikasi via email dibandingkan dengan kondisi bertatap muka. Dalam kondisi ini, pelaku BEC memiliki kontrol yang besar mengenai isyarat yang dikirimkan kepada korban. Terlebih, pelaku BEC telah memiliki seluruh informasi yang cukup terkait target korporasi atau individu yang akan disasar berikut segala informasi strategis yang perlu untuk diketahui.

Penjelasan terkait dengan upaya pelaku BEC memanipulasi citranya melalui email dapat dijelaskan dengan konsep penipuan digital (*digital deception*). Penipuan digital didefinisikan sebagai kontrol atas informasi yang disengaja dalam pesan yang dimediasi secara teknologi untuk menciptakan kepercayaan yang salah pada penerima pesan (Hancock & Gonzalez, 2013). Terdapat dua atribut utama dalam penipuan digital, yang meliputi kepercayaan yang salah (*false belief*) dan perihal intensionalitas. Pada pokoknya, penipuan digital memang dirancang untuk menipu, dan manusia selalu menjadi target awal dari para pelakunya tersebut (Loukas & Wilbanks, 2020).

Interpol menyebut bahwa secara umum BEC dilakukan dengan tiga tahap yang meliputi akses ilegal, rekaya sosial (*social engineering*), dan permintaan karena urgensi (Interpol, 2019). Proses manipulasi terjadi dalam tahapan rekayasa sosial, di mana pelaku BEC berhasil membuat korban termanipulasi dalam bentuk menyampaikan informasi penting bahkan melakukan pembayaran seperti yang diminta. Penipuan dalam bentuk digital yang diterima oleh korban dan rekayasa sosial yang dilakukan oleh pelaku membuat korban memiliki "persepsi ideal" tentang pengirim pesan. Dengan adanya sedikit isyarat yang diterima melalui email, korban penerima pesan BEC harus "mengisi kekosongan" atas ketidaklengkapan informasi yang dimiliki dan pada akhirnya cenderung mengasumsikan karakter positif atas citra dari pengirim pesan. Proses tersebut memicu adanya respons dalam bentuk umpan balik yang cenderung menyetujui apa yang diminta oleh pelaku BEC seperti digambarkan dalam skema di Gambar 5.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 5 *Computer-Mediated Communication* dalam Bentuk *Confirmatory Feedback* antara Pelaku dan Korban



Sumber: Teerakanok et al., (2020)

Proses ini diawali dengan upaya pelaku untuk memperoleh informasi lengkap terhadap korbannya. Dalam hal ini, pelaku melakukan berbagai cara seperti *hacking*, *phishing, malware, employee intrusion*, dan segala cara lainnya. Pelaku kemudian melakukan penipuan digital dalam bentuk rekayasa sosial hingga korban mempersepsikan pelaku dalam persepsi yang positif dan terbangun jalinan relasional yang terasa dekat. Dalam konteks *Computer-Mediated Communication*, pelaku bersama korban akan melalui fase interaksi impersonal, interpersonal, dan hiperpersonal. Setelahnya, korban akan menuruti instruksi pelaku untuk mentransfer sejumlah uang ke rekening yang sudah disiapkan. Pelaku kemudian melakukan praktik pencucian uang terhadap uang yang diterima, dan menghasilkan kerugian yang besar bagi korporasi yang menjadi targetnya. Dengan demikian, proses penipuan dengan skema BEC tidak lepas dari terbangunnya proses komunikasi melalui mediasi email.

Persuasi dalam BEC

Dalam perkembangannya, bentuk-bentuk BEC menjadi lebih bervariasi. Skema awal BEC yang bersifat impersonal, penyampaian level urgensi yang tinggi, dan bersifat otoritatif berkembang menjadi skema yang lebih komunikatif dan persuasif. Mulai masifnya kampanye anti-BEC terkait dengan penguatan infrastruktur teknologi informasi membuat pendekatan berbasis persuasi menjadi pilihan guna memanipulasi korban yang ditargetkan.

Biro Investigasi Federal Amerika Serikat (FBI) menyebutkan empat tahapan terjadinya BEC, yang meliputi (1) identifikasi target. Organisasi kriminal menargetkan korporasi bisnis di Amerika Serikat dan Eropa untuk mencari tahu segala jenis informasi strategis guna

mengembangkan proses presentasi diri yang selektif sesuai dengan karakter dari eksekutif perusahaan tersebut. Hal ini selaras dengan model komunikasi impersonal dalam *Computer-Mediated Communication*; (2) *grooming*. Di tahap ini, *email phishing* telah dilakukan dengan target kepada korban yang biasanya bekerja di bagian keuangan. Pelaku menggunakan pendekatan persuasif guna mengeksploitasi sifat alamiah manusia. Proses ini bisa terjadi dalam periode hitungan hari atau minggu; (3) pertukaran informasi. Di tahap ini korban telah berhasil diyakinkan oleh persuasi pelaku dan mulai memproses apa yang diminta oleh pelaku; dan (4) tranfer dana. Di tahap ini uang telah diterima oleh pelaku yang segera memutarnya dengan skema pencucian uang yang kompleks (FBI.gov, 2017).

Koordinator Kelompok Substansi Analisis dan Pemeriksaan Sektor Tindak Pidana Lainnya pada Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), Savetri Lihanara, menjelaskan adanya perkembangan dalam skema BEC bahwa komunikasi bersifat otoritatif di internal korporasi mulai digantikan dengan pola-pola yang lebih cenderung persuasif. Pola BEC kini lebih banyak terbangun antar mitra bisnis, yang membuatnya bergeser dari kecenderungan intimidatif dan sifat urgensi yang menyertainya. Dengan demikian, pola BEC dengan *email phishing* atas nama CEO suatu korporasi kepada pejabat atau staf yang dibawahinya tidak lagi menjadi bentuk yang lazim digunakan. Savetri menyebut komunikasi berbentuk persuasi dalam modus BEC dapat dilakukan karena pelaku sudah sangat memahami seluruh kebijakan internal, prosedur, budaya organisasi, hingga tutur bahasa yang dipakai dalam korporasi tersebut.

Praktik persuasi dalam BEC dapat dijelaskan dengan kerangka berpikir teori Model Kemungkinan Elaborasi. Richard Petty dan John Cacioppo mengembangkan model ini untuk mengeksplorasi bagaimana komunikator memproses pesan persuasif. Premisnya adalah manusia akan mengevaluasi pesan yang diterima dengan dua pilihan cara, baik melalui elaborasi kritis melalui rute sentral atau dengan pemikiran yang lebih sederhana melalui rute periferal. Pemilihan rute ini juga akan bermuara pada apakah terjadi perubahan sikap pada penerima pesan (Littlejohn et al., 2017).

Bila penerima pesan memilih rute sentral, pesan yang diterima akan melalui beberapa tahapan sebelum terjadinya perubahan sikap. Tahapan tersebut terdiri atas (1) motivasi. Tahap motivasi terdiri atas relevansi pesan secara personal dan adanya kebutuhan akan kognisi. Kebutuhan akan kognisi merupakan kenikmatan dalam memikirkan pesan- pesan yang diterima bahkan ketika pesan tersebut sesungguhnya tidak relevan secara pribadi; (2) kemampuan (*ability*). Tahap kemampuan ini meliputi kemampuan mengatasi distraksi dan adanya pemahaman yang memadai. Dalam tahapan ini dapat terjadi elaborasi objektif dan elaborasi bias; dan (3) kekuatan argumentasi. Argumentasi yang kuat akan mendorong perubahan sikap. Sedangkan argumentasi yang netral dan lemah tidak akan mengubah sikap, bahkan semakin memperkuat sudut pandang yang berlawanan (Littlejohn et al., 2017).

Sementara itu, rute periferal akan dipilih tanpa melalui elaborasi yang kompleks dan tanpa sejumlah tahapan yang harus dilalui. Rute ini hanya membutuhkan satu atau beberapa isyarat yang membuat perubahan sikap kemudian terjadi. Cialdini menyebut sejumlah isyarat seperti otoritas, komitmen, kontras, kelangkaan, timbal balik, kesukaan, bukti sosial, dan konsistensi. Isyarat lainnya dapat berupa imbalan nyata seperti makanan, uang, seks, atau berupa keahlian, penampilan, cara berbicara, latar belakang kredensial, kompetensi, karakter,

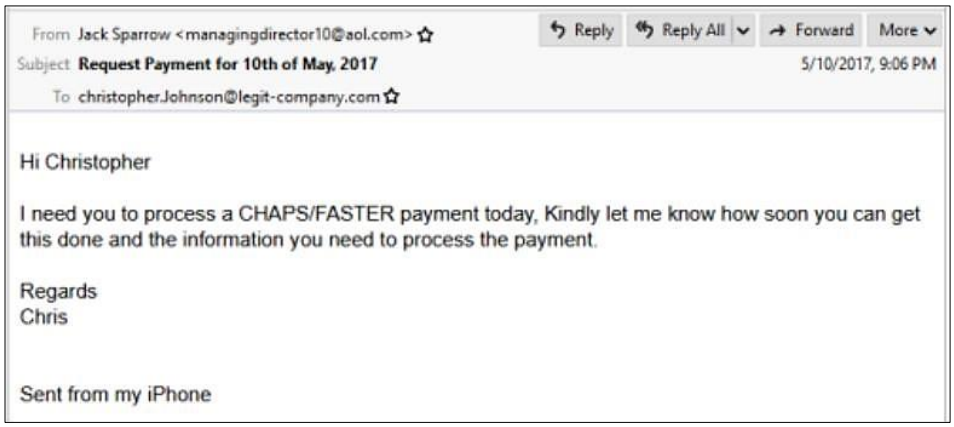
Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

prinsip kebajikan, perasaan simpatik, kesalahan tata bahasa, suasana hati, tipe komunikator, kredibilitas, dan berbagai isyarat lainnya (Dainton & Zelley, 2019). Rute periferal menjadi alternatif bagi komunikator untuk menjalankan persuasi kepada penerima pesan guna mengubah sikapnya. Namun, perubahan sikap dalam rute periferal cenderung bersifat sementara dan hanya dapat memenuhi kebutuhan yang bersifat jangka pendek.

Persuasi dalam BEC pada prinsipnya berupaya untuk mengarahkan korban sebagai penerima pesan dalam rute periferal. Rute ini dipilih mengingat BEC merupakan bentuk penipuan dengan tujuan utama meraih keuntungan yang diperoleh secara singkat. Bila penerima pesan menyadari telah mengalami penipuan, pelaku BEC telah menghilangkan jejaknya dan beralih pada pencarian target berikutnya.

Rute periferal dapat digunakan dengan bersandar pada satu atau sejumlah isyarat tertentu. Seperti saat kemunculan awal BEC, praktik otoritas sering digunakan dalam persuasi yang dilakukan. Bermodal kemampuan untuk meretas email atau memanipulasi alamat email CEO suatu perusahaan, persuasi BEC dapat dilakukan seperti dalam Gambar 6; isyarat kelangkaan dalam bentuk persuasi yang bersifat urgen seperti dalam Gambar 7; isyarat kontras di mana pelaku menempatkan diri dalam suatu rapat yang sangat penting sehingga proses pembayaran perlu dibantu oleh korban seperti di Gambar 8; atau isyarat dalam bentuk keahlian atau kredibilitas seperti dalam Gambar 9. Persuasi menggunakan rute periferal dengan sejumlah isyarat tertentu dapat mempercepat proses komunikasi dan mengubah sikap dari penerima pesan, yang membuat dalam beberapa temuan kasus BEC, transfer dana kepada rekening yang disediakan pelaku kejahatan begitu cepat dilakukan.

Gambar 6 Persuasi dalam BEC dengan Menggunakan Isyarat Otoritas


From Jack Sparrow <managingdirector10@aol.com>
Reply | Reply All | Forward | More
Subject **Request Payment for 10th of May, 2017**
5/10/2017, 9:06 PM
To christopher.Johnson@legit-company.com

Hi Christopher

I need you to process a CHAPS/FASTER payment today, Kindly let me know how soon you can get this done and the information you need to process the payment.

Regards
Chris

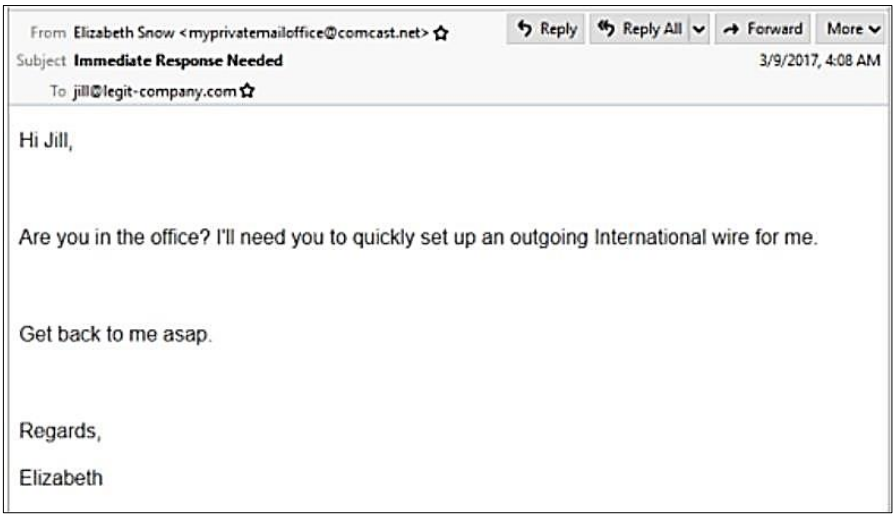
Sent from my iPhone

Sumber: FBI, 2017

Dengan memanipulasi kesan sebagai atasan dari pegawai yang khususnya bekerja di bidang administrasi keuangan, pelaku BEC dapat mengarahkan korban untuk dapat segara menjalankan apa yang diminta. Mengingat instrumen komunikasi menggunakan email adalah hal yang biasa dalam operasioanl suatu organisasi atau perusahaan, pegawai akan menjalankan perintah dari bos atau atasan tanpa berpikir panjang dan mengklarifikasi kebenaran identitas dari pemilik email tersebut.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 7 Persuasi dalam BEC dengan Menggunakan Isyarat Kelangkaan



Sumber: FBI, 2017

Menggunakan isyarat kelangkaan menjadi tipikal dalam proses persuasi yang membuat korban akan menjalankan perintah tanpa melalui proses berpikir yang optimal. Penggunaan isyarat kelangkaan ini lazimnya dibarengi dengan perintah untuk menjalankan kemauan pelaku BEC agar proses tidak melalui proses yang normal dan memakan waktu, namun bisa dieksekusi sesegera mungkin tanpa harus dipertanyakan lagi.

Gambar 8 Persuasi dalam BEC dengan Isyarat Kontras

Sumber: FBI, 2017

Isyarat kontras dijalankan oleh pelaku guna menyentuh jalur periferal calon korbannya. Sebagai contoh seperti dalam Gambar 8, pelaku mencoba membuat korban memahami kesibukan yang sedang dijalani dengan berbagai tugas secara bersamaan. Dengan demikian, tugas yang dimintakan kepada korban seperti dalam bentuk transfer sejumlah uang kepada pelaku diharapkan tidak perlu dipertanyakan secara rinci.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 9 Persuasi dalam BEC dengan Isyarat Keahlian/Kredibilitas

Sumber: FBI, 2017

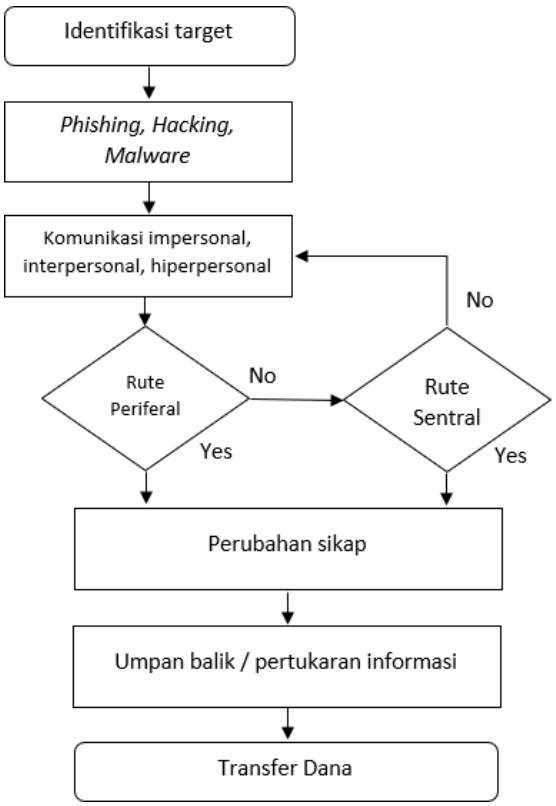
Modus lain dalam BEC adalah ketika pelaku berupaya memanipulasi dengan cara menyanjung kredibilitas dan kompetensi korban. Pujian menjadi instrumen yang ampuh kepada sejumlah orang yang akan memberi kerja terbaiknya ketika diberikan sanjungan dan apresiasi. Kebanggaan atas pujian yang diperoleh membuat korban tidak menjalankan proses kognitif secara memadai dan secara sukarela menjalankan apa yang diperintahkan oleh pelaku.

Dalam praktiknya, pelaku BEC tidak semata mengarahkan proses persuasi ke rute periferal, karena ditemuinya perbedaan respons dari target atau korbannya dalam menyikapi pesan yang diterima oleh pelaku. Savetri Lihanara dari PPATK menyebutkan bahwa modus terkini dari BEC adalah pengubahan nama korporasi oleh pelaku dengan menggunakan nama PT berbahasa Indonesia. Hal ini mengubah pola saat pelaku dahulunya masih menggunakan nama korporasi berskala internasional yang berbentuk Ltd. Dalam konteks inilah, pelaku akan menjelaskan dengan rinci mengapa terjadi perubahan nama korporasi dalam email yang disampaikan kepada mitra bisnis yang menjadi korban, dan butuh waktu bagi korban untuk memahami komunikasi dan persuasi yang dilakukan oleh pelaku. Dalam konteks ini, pelaku membangun tahapan motivasi dan kognisi yang relevan, membangun kemampuan dan pemahaman bisnis yang memadai, serta membangun argumentasi yang kuat. Savetri Lihanara menyebut bahwa pengubahan nama korporasi berikut alamat rekening kepada mitra bisnis yang menjadi korban relatif berhasil, karena proses komunikasi dan persuasi yang dijalankan berhasil mengubah sikap korbannya untuk kemudian melakukan pembayaran kepada pelaku. Dalam tahapan BEC yang dijelaskan oleh FBI seperti yang telah dijelaskan, proses komunikasi yang dijalin antara pelaku dan korban dalam BEC bisa membutuhkan waktu beberapa hari atau beberapa minggu. Bila ditemukan kondisi rute sentral tidak menghasilkan perubahan sikap pada korban, pelaku BEC akan kembali mengulang proses komunikasi dari awal dengan kembali berproses pada rute periferal.

Berdasarkan penjelasan yang diperoleh dari temuan studi dokumentasi dan wawancara, dapat digambarkan model komunikasi dan persuasi dari praktik penipuan dengan modus *Business Email Compromise* (BEC) sebagai berikut:

Jurnal Riset Komunikasi JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Gambar 10 Model Komunikasi dan Persuasi dalam *Business Email Compromise*



Sumber: Olahan Peneliti, 2022

Model tersebut menggambarkan bahwa komunikasi dalam *Business Email Compromise* dibangun setelah proses pengumpulan informasi, manipulasi digital (*hacking, phishing, malware*), dan penentuan target telah selesai dilaksanakan. Awal komunikasi dibangun dengan bentuk impersonal karena terkait dengan proyek pekerjaan, sebelum bergeser ke tahapan interpersonal dan hiperpersonal. Proses persuasi dijalankan setelah komunikasi hiperpersonal terjalin, dengan upaya untuk mengarahkan pada rute periferal. Rute periferal diimplementasikan dengan satu atau beberapa isyarat tertentu, seperti otoritas, kompetensi, urgensi, kredibilitas, dan lainnya. Pelaku BEC juga menyiapkan alternatif skenario memasuki rute sentral jika korban tidak serta merta mengalami perubahan sikap dalam penggunaan rute periferal. Bila persuasi yang memakan waktu beberapa hari atau beberapa minggu masih gagal mengubah persepsi korban, maka pelaku akan kembali menjalankan komunikasinya sejak awal hingga tercapainya tujuan yang ditetapkan.

PENUTUP

Penipuan dengan modus BEC pada umumnya dijalankan dengan menggunakan mediasi komputer, khususnya email. Penggunaan email dari pelaku kepada korban menciptakan proses terjadinya komunikasi impersonal yang bersifat profesional, kemudian mengarah kepada komunikasi interpersonal yang ditandai dengan peningkatan aktivitas komunikasi, hingga komunikasi hiperpersonal karena korban merasa sudah mengenal dekat dan mempercayai pelaku walaupun hanya melalui perantara email.

Perkembangan fase dari impersonal hingga interpersonal tersebut tidak lepas dari upaya persuasi yang dibangun dalam narasi email yang dikirimkan. Pada umumnya, pelaku akan berupaya mempersuasi korban melalui isyarat-isyarat periferal yang ringan, seperti dalam bentuk isyarat otoritas, isyarat kelangkaan, isyarat kontras, hingga isyarat keahlian/kredibilitas. Ketika korban menjalankan proses kognitif dan mempertanyakan tujuan pelaku, pelaku akan kembali mengarahkan korban ke dalam rute periferal dengan sejumlah isyarat ringan yang menarik perhatian perilaku. Bahkan meskipun korban tetap bertahan di rute sentral, pelaku BEC akan tetap mencoba membangun komunikasi dengan indikator-indikator di rute sentral yang meliputi motivasi, kemampuan, dan argumentasi.

BEC menjadi problematika tidak hanya di Indonesia, karena praktiknya kejahatan ini bersifat transnasional. Upaya mengatasinya harus dibangun secara komprehensif dengan melibatkan berbagai perspektif terkait seperti hukum dan regulasi, ekonomi dan audit, teknologi informasi, hingga pemahaman komunikasi. Koordinasi antara seluruh pemangku kepentingan dengan pemahaman yang sama dan utuh juga sangat krusial agar kejahatan dengan modus BEC tidak semakin berkembang.

Sebagai pencegahan, upaya pendirian usaha melalui *One Single Submission* (OSS) harus melalui verifikasi yang memadai, khususnya di level Pemerintah Daerah yang memiliki kewenangan tersebut. Pemantauan terhadap Badan Usaha yang telah terdaftar namun tidak beraktivitas juga harus dilakukan agar tidak dijadikan sebagai sarana kejahatan. Bagi perbankan, selain penguatan pemahaman mengenai pola komunikasi dan persuasi bagi petugasnya, dapat memperketat proses *Know Your Customer* dan menjalankan *Enhance Due Diligence* terhadap transfer masuk yang signifikan dari luar negeri kepada rekening yang baru dibuka. Dari aspek pemberantasan, penguatan kapasitas penegak hukum dan membangun Kerja sama antara seluruh pemangku kepentingan terkait di dalam dan luar negeri juga perlu ditingkatkan, dengan melibatkan optimalisasi peran Kedutaan Besar RI di berbagai negara, jaringan intelijen keuangan global, hingga jejaring koordinasi penegak hukum antarnegara.

Penelitian lanjutan terkait dengan BEC dalam konteks komunikasi dapat dikembangkan dengan pendekatan observasi partisipatif, khususnya bila peneliti memiliki akses langsung dalam proses penanganan BEC yang melibatkan penegak hukum. Penelitian ke depan juga perlu menjalankan wawancara terhadap korban BEC guna memperkuat data penelitian dengan mendapatkan perspektif langsung dari korban yang merupakan sumber primer.

REFERENSI

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analyzing Cyber Crimes during COVID-19 Time in Indonesia. *3rd International Conference on Computer Communication and the Internet*, 78–83.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. California: Praeger.

Business Email Compromise. (2017). Tersedia dari https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Business Email Compromise Fraud. (2019). Tersedia dari https://www.interpol.int/Crimes/Financial-crime/Business-Email-Compromise-Fraud

Carr, C. T. (2021). *Computer-Mediated Communication: A Theoretical and Practical Introduction to Online Human Communication* (1st Edition). Maryland: Rowman & Littlefield Publishers.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. London: SAGE Publications.

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *27*(3), 871–884. https://doi.org/10.1108/JFC-02-2020-0026

Dainton, M., & Zelley, E. D. (2019). *Applying Communication Theory for Professional Life: A Practical Introduction* (4th Editio). California: Sage Publications.

Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian RI. (2020). *Membedah Tindak Pidana Siber sebagai Tindak Pidana Asal TPPU*. Jakarta: Direktorat Tindak Pidana Siber Badan Reserse Kriminal Kepolisian RI

Ean, L. C. (2011). Computer-mediated communication and organisational communication: the use of new communication technology in the workplace. *SEARCH Journal of the Southeast Asia Research Centre for Communications and Humanities*, *3*(1), 1–12.

FBI Tindak Lanjuti Kasus Website Palsu yang Bobol Data 30 Ribu Warga AS. (2021). Tersedia dari https://news.detik.com/berita-jawa-timur/d-5538022/fbi-tindak-lanjuti-kasus-website-palsu-yang-bobol-data-30-ribu-warga-as?single=1

Griffin, E., Ledbetter, A., & Sparks, G. G. (2018). A First Look At Communication Theory, 10th Edition. In *McGraw-Hill*. (Tenth Edit). New York: McGraw Hill Education.

Hancock, J., & Gonzalez, A. (2013). Deception in computer-mediated communication. In *Pragmatics of Computer-Mediated Communication* (pp. 363–386).

Hidayat, M. (2017). Model Komunikasi Kyai Dengan Santri di Pesantren. *Jurnal ASPIKOM*, *2*(6), 385. https://doi.org/10.24329/aspikom.v2i6.89

Juditha, C. (2015). Pola Komunikasi Dalam Cybercrime (Kasus Love Scams). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *6*(2), 122582.

Juditha, Christiany. (2018). Interaksi Simbolik Dalam Komunitas Virtual Anti Hoaks Untuk Mengurangi Penyebaran Hoaks. *Jurnal PIKOM (Penelitian Komunikasi dan Pembangunan)*, *19*(1), 17. https://doi.org/10.31346/jpikom.v19i1.1401

Kusmarni, Y. (2012). Studi Kasus. *Jurnal Edu UGM Press*.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*(0), 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International*

Journal of Criminal Justice Sciences, *12*(2), 196–207. https://doi.org/10.5281/zenodo.1034658

Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber crime. *International Journal of Cyber Criminology*, *9*(2), 185–204. https://doi.org/10.5281/zenodo.56225

Littlejohn, S. W., Foss, K. A., & Oetzel, J. G. (2017). *Theories of Human Communication* (Eleventh E). Waveland Press.

Loukas, G., & Wilbanks, L. R. (2020). Digital Deception : Cyber Fraud and Online Misinformation. *IT Professional*, *22*(April), 19–20. https://doi.org/10.1109/MITP.2020.2980090

Muzaini. (2014). Perkembangan Teknologi dan Perilaku Menyimpang dalam Masyarakat Modern. *Jurnal Pembangunan Pendidikan: Fondasi Dan Aplikasi*, *2*(1), 48–58.

Nurahma, G. A., & Hendriani, W. (2021). Tinjauan sistematis studi kasus dalam penelitian kualitatif. *Mediapsi*, *7*(2), 119–129.

Pitts, V. (2017). *Cyber Crimes: History of World's Worst Cyber Attacks*. Alpha Editions.

Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia. (2018). Tersedia dari https://kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media

PPATK ingatkan meningkatnya kejahatan siber dengan skema BEC. (2021). Tersedia dari https://www.antaranews.com/berita/2335102/ppatk-ingatkan-meningkatnya-kejahatan-siber-dengan-skema-bec

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016*. https://doi.org/10.1109/ICCCF.2016.7740434

Saud Al-Musib, N., Mohammad Al-Serhani, F., Humayun, M., & Jhanjhi, N. Z. (2021). Business email compromise (BEC) attacks. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2021.03.647

Setiawan, Y., Zulkarnain, & Nurjanah. (2020). Pengaruh komunikasi berbasis komputer terhadap kualitas pelayanan perpustakaan di perpustakaan universitas riau. *Jurnal Riset Komunikasi*, *3*(1), 1–15.

Shahbazi, A. (2019). Technological developments in cyberspace and commission of the crimes in international law and Iran. *Journal of Legal, Ethical and Regulatory Issues*, *22*(4), 1–12.

Sugiyono. (2009). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Alfabeta.

Teerakanok, S., Yasuki, H., & Uehara, T. (2020). A Practical Solution against Business Email Compromise (BEC) Attack using Invoice Checksum. *Proceedings - Companion of the 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security, QRS-C 2020*, 160–167. https://doi.org/10.1109/QRS-C51114.2020.00036

Walther, Joseph, B. (1996). Computer-Mediated Communication: Impersonal, Interpersonal and Hyperpersonal Interaction. *Communication Research* (Vol. 23, Issue 3, pp. 3–43).

Walther, J. B. (2011). Theories of CMC and interpersonal relations. *The Handbook of Interpersonal Communication*, *4*, 443–479.

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Sage Publications.

Jurnal Riset Komunikasi
JURKOM
P-ISSN: 2615-0875
E-ISSN: 2615-0948

Zweighaft, D. (2017). Business email compromise and executive impersonation: are financial institutions exposed? *Journal of Investment Compliance*, *18*(1), 1–7. https://doi.org/10.1108/joic-02-2017-0001