NCAF PROCEEDING OF NATIONAL CONFERENCE ON ACCOUNTING & FINANCE

Volume 5, 2023 Hal. 176-183

Analisa pola sosialisasi pencegahan modus *social engineering* melalui media website dan twitter

Rahmadani Ningtyas Sekar Putri, Hendi Yogi Prabowo

Universitas Islam Indonesia
Email: 20919008@students.uii.ac.id

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi pola sosialisasi pencegahan social engineering melalui media website dan twitter enam bank besar di Indonesia. Penelitian kualitatif ini menggunakan metode archival research dan menggunakan data documentary secondary yaitu menggunakan media website dan twitter milik bank. Data penelitian diolah menggunakan Software NVivo 12. Hasil penelitian menunjukkan bahwa sosialisasi pencegahan social engineering yang diberikan oleh enam bank di Indonesia melalui media website dan twitter memuat informasi mengenai ciri-ciri social engineering, sarana layanan kontak bank, serta memberikan langkah-langkah pencegahan. Sosialisasi yang diberikan melalui media website lebih informatif, sedangkan sosialisasi melalui twitter memberikan informasi yang singkat, karena ada batasan karakter pada postingan twitter. Optimalisasi sosialisasi melalui website dan twitter dapat dilakukan dengan cara membuat konten yang memuat informasi secara lengkap dan terkini mengenai ciri-ciri penipuan, sarana layanan kontak, dan langkah-langkah pencegahan yang dapat divisualisasikan dalam bentuk video atau gambar poster yang di desain dengan menarik.

Kata Kunci: Penipuan Social Engineering, Sosialisasi Pencegahan, Twitter, Website.

DOI: 10.20885/ncaf.vol5.art20

PENDAHULUAN

Gibbs (2020) mengatakan meningkatnya kejahatan siber disebabkan pesatnya perkembangan teknologi. Menurut Kävrestad (2018) kejahatan siber terbentuk karena adanya sarana dan peluang yang kemudian akan melibatkan alat dan pengetahuan yang sudah terkomputerisasi. Pelaku dapat melakukan berbagai kejahatan dengan teknik dan metode yang berbeda di dunia maya, khususnya di dunia perbankan seperti *phising, vishing*, mengindetifikasi pencurian, penolakan layanan, *social engineering*, dan lain nya yang bertujuan untuk mencuri data keuangan nasabah (Ali, 2019).

Badan Siber dan Sandi Negara (2020) mengatakan pada tanggal 1 Januari hingga 12 April 2020 tercatat sebesar 88.414.296 serangan siber terjadi, yang berjenis *Malicious Email Phising* dengan isu pandemi *Covid-19* sebagai latar belakang penyerangan. Serangan ini disebut s*ocial engineering*, yaitu serangan psikologis yang menyerang manusia dengan cara menipu yang dapat mengakibatkan kerugian keuangan, pencurian identitas, dan manipulasi data. Hasan & Febriany (2021) mengatakan maraknya perkembangan digital dan teknologi yang semakin canggih memiliki dampak positif dan juga negatif bagi dunia perbankan, dan semakin banyak juga kejahatan dari segi finansial, sehingga diperlukan langkah pencegahan dan penanganan. Pencegahan *social engineering* di sektor bank dapat dilakukan dengan berbagai cara seperti memperbaiki sistem bank, mengoptimalkan pengetahuan karyawan, serta memberikan sosialisasi kepada nasabah. Cara pencegahan dengan memberikan sosialisasi kepada nasabah memiliki tingkat urgensi yang lebih tinggi, karena banyak yang menjadi korban serangan *social engineering* adalah nasabah bank, sehingga nasabah merupakan hal penting yang harus dilindungi.

Kini pemberian sosialisasi pencegahan *social engineering* kepada nasabah secara *online* lebih mudah, karena pemberian sosialisasi secara *online* dapat dibagikan secara luas. Berdasarkan data dari *We Are Social* tahun 2022 tercatat 204,7 juta pengguna yang menggunakan internet dan 191,4 juta pengguna media sosial aktif dari total jumlah penduduk 277,7 juta orang. Adapun *platform* media sosial yang sering digunakan masyarakat yaitu twitter, dengan pengguna twitter sebanyak 58,3% dari jumlah penduduk. Sosialisasi pencegahan penipuan *social engineering* melalui media website dan media sosial twitter merupakan langkah

yang tepat, karena sosialisasi dapat dibagikan secara luas. Oleh karena itu, peneliti tertarik untuk menganalisa pencegahan *sosial engineering* dengan memaparkan pola-pola sosialisasi enam bank besar di Indonesia melalui media website dan twitter. Adapun bank-bank besar tersebut diantaranya Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, dan Bank Syariah Indonesia (BSI).

TINJAUAN LITERATUR

Consumer Fraud

Consumer Fraud didefinisikan sebagai praktik bisnis menipu yang dapat menyebabkan konsumen mengalami kerugian finansial atau kerugian lainnya. Menurut Titus, R. M. & Gover (2001) korban menjadi "fasilitas" dalam penipuan ini, secara tidak langsung membantu pelaku dalam melakukan tindakan penipuan. Adapun jenis penipuan *consumer fraud* yang sering terjadi diantaranya penipuan produk, promosi hadiah palsu, ditagih untuk membeli walaupun dalam posisi tidak setuju, ditagih pembelian layanan internet yang tidak disetujui pembelian nya, dan penipuan program kerja di rumah (Anderson, 2011).

Social Enggineering Attack

Chetioui et al. (2022) mengatakan *social engineering* adalah seni dalam mempengaruhi suatu invidu untuk mendapatkan informasi rahasia seperti kata sandi, alamat, informasi detail yang berkaitan dengan bank. Keberhasilan dari serangan *social engineering* tentunya memiliki langkah yang tepat bagi penyerang untuk melakukan aksinya. Chetioui et al. (2022) juga mengatakan terdapat empat langkah dalam siklus *social engineering* diantaranya *investigation*, *hook*, *play*, *exit.*

Gullibility

G*ullibility* dapat didefinisikan sebagai kecenderungan yang tidak biasa untuk ditipu atau dimanfaatkan. Menurut Greenspan (2008) terdapat empat faktor yang berkontribusi dalam hal mudahnya orang tertipu diantaranya: (1) Situasi, mungkin penipu sangat persuasif, atau mungkin ada orang lain yang menjamin kejujurannya; (2) Kognisi, mungkin korban tidak dapat membaca sikap penipu atau tidak mengetahui jenis investasi yang dicakup oleh *scam; (3)* Kepribadian, mungkin korban adalah orang yang sangat dipercaya atau sulit mengatakan 'tidak'; (4) Keadaan, mungkin korban kelelahan atau dalam keadaan mabuk atau sangat tergantung dengan penipu.

Crime Triangle of Routine Activity Theory

Cohen & Felson (1979) terdapat tiga elemen dimana peristiwa kejahatan itu terjadi, sebagaimana ketiga elemen ini harus menyatu dalam konteks tempat atau waktu yang sama diantaranya *offender* (pelaku), *target* (korban)*, place* (tempat). Sementara untuk segitiga kejahatan versi terbaru, terdapat segitiga di lapisan luar yaitu *guardian, handler,* dan *manager* yang hal ini berfungsi sebagai *controllers* dari setiap elemen segitiga kejahatan yang berada di lapisan dalam (Eck 2003). Posisi *controllers* memiliki peran penting dalam mencegah terjadinya kejahatan serta memiliki tanggung jawab terhadap elemen-elemen yang ada di lapisan bagian dalam segitiga kejahatan *(crimes triangle).* Jika dikaitkan teori *crime triangle* dengan penelitian ini, keberadaan *controllers* diibaratkan sebagai pihak bank yang memiliki peran penting untuk mengatasi modus *social engineering* pada nasabah bank.

Media Sosialisasi

Website

Menurut Hasugian (2018) website mampu memberikan informasi menjadi lebih efisien dan ter-*update.* Balzer et al. (2020) mengatakan aplikasi web bertujuan untuk mengeksplorasi hubungan seluruh kumpulan data yang besar dan kompleks dengan mudah, cepat, dan interaktif. Website memiliki fungsi yang lebih luas dengan pengoptimalan dari segi isi atau konten di halaman web, agar artikel yang diunggah memiliki daya ketertarikan bagi orang yang membacanya.

Twitter

Twitter merupakan sebuah *platform* media sosial yang mengkombinasikan media jejaring sosial dan *microblog*. Pada tanggal 7 November 2017 penggunaan teks yang digunakan hingga 280 karakter twit. Lewat twitter juga seseorang dapat membalas pesan atau *reply,* atau meneruskan pesan dengan format kata *"retweet"* atau "RT". Sebutan *trending topics* menjadi sebuah ukuran seberapa berhasilnya penyebaran informasi dalam media tersebut yaitu ditunjukkan dengan banyaknya yang me-*retweet, reply,* atau *mention*. Informasi dapat tersebar secara luas dan cepat melalui twitter karena fitur *retweet* yang dimilikinya (Iryanti & Rahman, 2019).

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif. Metode yang digunakan adalah *archival research*. Saunders, dkk. (2012) mendifinisikan *archival research* sebagai strategi penelitian yang menggunakan catatan dan dokumen sebagai sumber utama yang dihasilkan dari aktivitas sehari-hari. Peneliti mengumpulkan informasi secara lengkap dan mendalam mengenai sosialisasi pencegahan penipuan *social engineering* yang dilakukan bank-bank besar di Indonesia melalui media website dan twitter resmi bank.

Penelitian ini bertujuan untuk menganalisa pola-pola sosialisasi pencegahan modus *social engineering* oleh bank melalui media website dan twitter. Penelitian ini menggunakan *secondary data* yang sifatnya *documentary* diantaranya media website dan media sosial twitter bank sebagai media untuk mengumpulkan data. Data diambil dengan periode waktu bulan Januari hingga Februari 2022 dengan menggunakan fitur *Ncapture* untuk men-*capture* konten yang terdapat di website dan media sosial twitter. Adapun website dan media sosial twitter yang dijadikan data dalam penelitian ini adalah bank-bank besar di Indonesia yang memiliki aset besar yang tercatat oleh OJK dan Bank Indonesia diantaranya Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, dan Bank Syariah Indonesia (BSI).

Selanjutnya dalam menganalisis data, peneliti mengacu pada model data Miles & Humberman (1994). Pertama, *coding* yaitu mengidentifikasi, memberi label, dan mensistematisasikan data sebagai milik atau mewakili beberapa jenis fenomena (Tracy, 2013). Kedua, tampilan data yang menggunakan tampilan *analytical maps* dan *matrix coding query*. Ketiga, menarik kesimpulan atas hasil analisis data dan menilai implikasi dari sebuah makna yang timbul dari pertanyaan-pertanyaan yang terjadi selama proses penelitian. Kemudian, data yang telah terkumpul dianalisis menggunakan pendekatan *content analysist* dan diuji keabsahannya menggunakan tringulasi sumber yang berfokus pada data yang diperoleh dari berbagai sumber.

HASIL DAN DISKUSI

Dalam menyajikan hasil penelitian, peneliti mengacu pada hasil analisis konten, yang telah diolah peneliti dari hasil *NCapture* website dan twitter bank yang kemudian dilakukan pengkodean melalui bantuan *Software NVivo 12*. Berikut ini hasil pengkodean data dan hasil analisis yang dapat dilihat pada gambar 1.

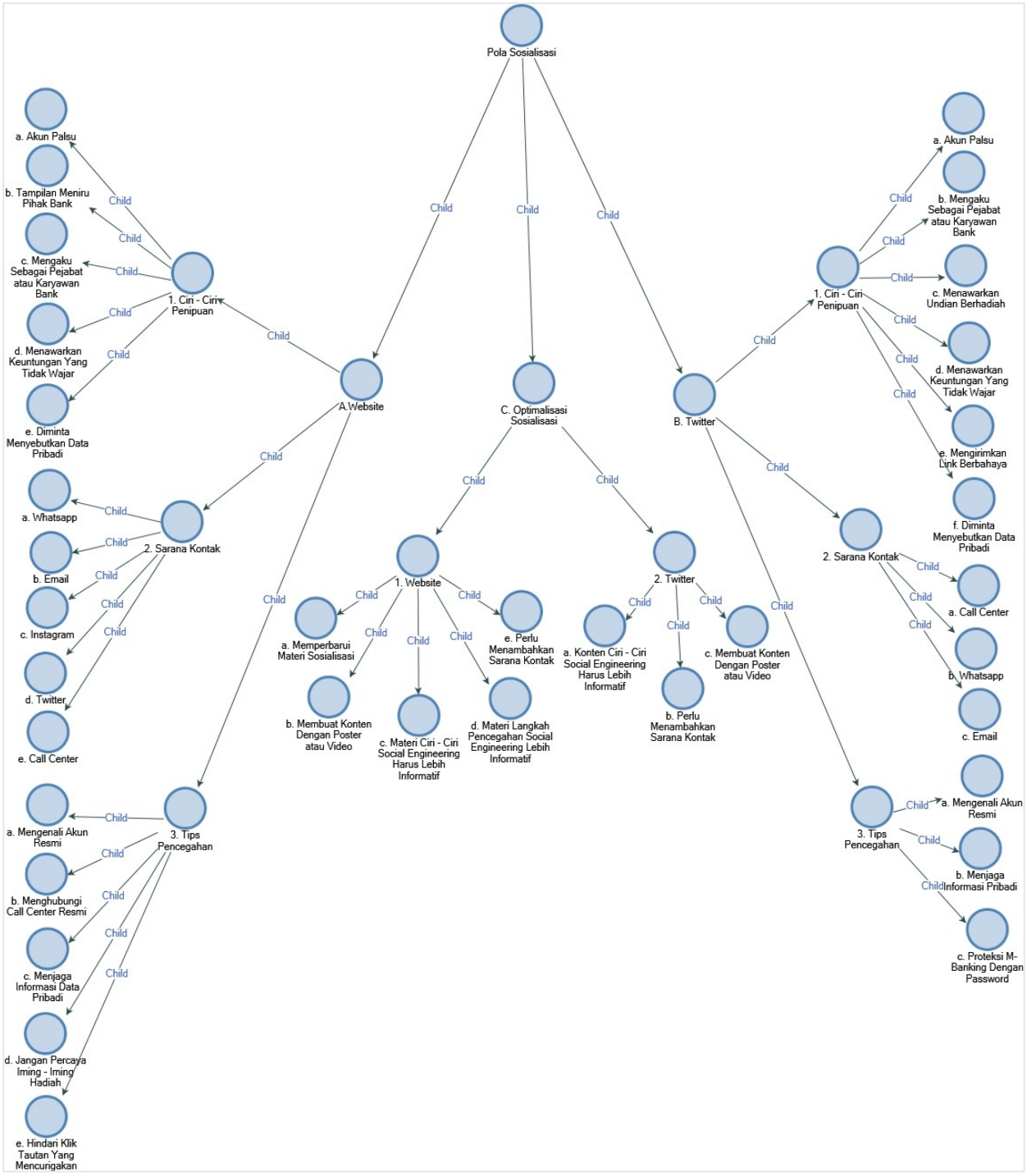
Berdasarkan gambar peta analisa di atas, maka hasil penelitian yang berkaitan dengan pola-pola sosialisasi dalam rangka melakukan pencegahan *social engineering* dapat dilihat pada uraian-uraian di bawah ini:

Sosialisasi Pencegahan *Social Engineering* Oleh Bank Melalui Website

Informasi yang diberikan dalam sosialisasi pencegahan *social engineering* melalui website Bank Central Asia (BCA), Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI), Bank Permata, dan Bank Syariah Indonesia (BSI) diantara nya: mengenali ciri-ciri penipuan, layanan sarana kontak, langkah-langkah pencegahan *social engineering*.

Berdasarkan hasil *coding* pada tabel 1, memberikan keterangan "angka" yang mengartikan bahwa banyaknya kata yang sering muncul dari poin-poin sosialisasi pencegahan *social engineering* melalui website. Sosialisasi pencegahan modus *social engineering* yang diberikan oleh keenam bank tersebut, umumnya memberikan himbauan kepada nasabah untuk menjaga informasi data pribadi. Pada tabel 1 memuat

beberapa informasi, diantaranya: (1) Ciri-ciri modus *social engineering* yang paling banyak disampaikan dalam sosialisasi yaitu mengaku sebagai pejabat atau karyawan bank, yang hal ini disampaikan oleh BRI dengan jumlah kata yang disebut 244 kata; (2) Sarana kontak yang paling banyak dicantumkan dalam media website bank yaitu kontak whatsapp, sebagaimana yang disampaikan oleh BRI dengan jumlah kata yang disebut 305 kata; (3) Tips pencegahan modus *social engineering* yang sering di sosialisasikan yaitu mengenali akun resmi, sebagaimana yang disosialisasikan oleh BCA dengan jumlah kata yang disebut 505 kata.



Sumber: Diolah Peneliti Menggunakan *NVivo* 12

Gambar 1. Peta Analisis Pola-Pola Sosialisasi Pencegahan *Social Engineering* Pada Nasabah Perbankan

Tabel 1. *Matrix Coding* Sosialisasi Pencegahan *Social Engineering* Melalui Website[1]

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

Sumber: Diolah Peneliti Menggunakan *NVivo* 12

Sosialisasi pencegahan *social engineering* melalui media website yang dilakukan oleh keenam bank tersebut masih belum optimal, diantaranya: (1) Bank Mandiri, BNI, BSI tidak meng-*upgrade* informasi mengenai sosialisasi pencegahan, sehingga informasi yang diberikan masih dengan isu yang lama serta pencegahannya pun masih dengan cara yang lama; (2) Konten sosialisasi melalui website, perlu menampilkan bacaan yang menarik seperti menggunakan poster atau video yang memiliki visualisasi yang unik; (3) Keenam bank tersebut tidak memberikan sosialisasi secara lengkap mengenai ciri-ciri *social engineering* dan langkah-langkah pencegahan; (4) Sosialisasi sarana kontak yang diberikan oleh BNI melalui website belum lengkap.

Sosialisasi Pencegahan *Social Engineering* Melalui Twitter

Postingan twit yang dibuat oleh bank mengenai penipuan *sosial engineering* memberikan informasi mengenai ciri-ciri modus *social engineering*, sarana kontak, serta langkah-langkah pencegahan. Namun, terdapat perbedaan sosialisasi melalui website dan twitter, yaitu twitter didominasi informasi yang memiliki kalimat pendek, karena ada batasan twit 280 karakter. Berikut ini peneliti akan memaparkan pola-pola sosialisasi bank dalam pencegahan penipuan *sosial engineering* yang diberikan melalui twitter.

Berdasarkan hasil c*oding* pada tabel 2, memberikan keterangan "angka" mengartikan bahwa banyaknya kata yang sering muncul dari poin-poin sosialisasi pencegahan *social engineering* melalui twitter. Pada tabel 2 memuat beberapa informasi, diantaranya: (1) Ciri-ciri modus *social engineering* yang paling banyak disosialisasikan yaitu mengaku sebagai pejabat atau karyawan bank, yang hal ini disampaikan oleh Bank Mandiri dengan jumlah kata yang disebut 3298 kata; (2) Sarana kontak yang paling banyak dicantumkan dalam media twitter bank yaitu kontak whatsapp, sebagaimana yang disampaikan oleh BNI dengan jumlah kata yang disebut yaitu 1192 kata; (3) Tips pencegahan modus *social engineering* yang sering disosialisasikan yaitu mengenali akun resmi dan menjaga informasi pribadi, sebagaimana yang disosialisasikan oleh Banj Mandiri dengan jumlah kata yang disebut 3299 kata dan 3315 kata.

[1] Berdasarkan jumlah kata

Tabel 2. *Matrix Coding* Sosialisasi Layanan Sarana Kontak Melalui Media Twitter[2]

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

Sumber: Diolah Peneliti Menggunakan *NVivo*

Sosialisasi pencegahan modus *social engineering* melalui media twitter yang dilakukan oleh Bank Mandiri, Bank Central Asia (BCA), Bank Rakyat Indonesia (BRI), Bank Negara Indonesia (BNI), Bank Permata dan Bank Syariah Indonesia (BSI) masih belum optimal, berikut diantaranya: (1) Tidak memberikan informasi yang lengkap mengenai ciri-ciri *social engineering* seperti BCA, BNI, BRI, Bank Mandiri dan Bank Permata yaitu tidak memasukan modus menawarkan undian berhadiah sebagai ciri-ciri modus *social engineering*; (2) Sosialisasi yang diberikan BCA, BNI, BRI, Bank Permata tidak menyediakan sarana kontak *email*. Layanan sarana kontak *email* juga tak kalah penting, karena *email* dapat membantu nasabah untuk mengirim dokumen yang banyak kepada bank dan memiliki fleksibelitas dalam berkomunikasi dengan orang lain. (3) Sosialisasi yang dilakukan oleh BNI melalui media twitter masih monoton, karena postingan twitnya didominasi dengan teks tanpa ada gambar ataupun video.

Optimalisasi Media Website Milik Bank Dalam Pencegahan *Social Engineering*

Bank harus memberikan sosialisasi yang informatif dan bermanfaat bagi nasabahnya supaya sosialisasi melalui website tersampaikan dengan baik dan optimal, sehingga diperlukan beberapa perbaikan dalam menyampaikan sosialisasi pencegahan modus *social engineering* melalui media website, diantaranya: (1) Sosialisasi pencegahan modus *social engineering* yang dibagikan melalui Bank Mandiri, BNI, BSI perlu meng-*update* materi sosialisasinya. Hal ini dikarenakan serangan *social engineering* tiap tahunnya muncul jenis serangan baru dan ditambah teknologi semakin berkembang, sehingga diperlukan juga cara-cara mencegah serangan *social engineering* dengan jenis baru; (2) Perlu bagi BCA, BNI, Bank Mandiri, BSI untuk mengoptimalkan sosialisasi pencegahan *social engineering* dengan membuat konten gambar poster atau video yang menarik minat nasabah untuk melihat; (3) Sosialisasi yang diberikan oleh keenam bank tersebut harus memuat informasi yang lengkap mengenai ciri-ciri modus *social engineering* dan langkah-langkah pencegahannya; (4) Perlu bagi BNI untuk mencantumkan media sosial dan *email* BNI, karena saat ini banyak nasabah yang mengakses media sosial dan email di kehidupan sehari-harinya.

Optimalisasi Media Twitter Milik Bank Dalam Pencegahan *Social Engineering*

Adapun perbaikan yang perlu dilakukan oleh bank-bank terkait dengan sosialisasi pencegahan *social engineering* melalui media twitter, diantaranya: (1) Sosialiasi mengenai ciri-ciri *social engineering* yang diberikan oleh BCA, BNI, BRI, Bank Mandiri dan Bank Permata perlu menambahkan modus menawarkan undian

[2] Berdasarkan jumlah kata

berhadiah, karena modus seperti ini sering terjadi agar korban mau menyerahakan informasi pribadi ke pelaku; (2) Bagi BCA, BNI, BRI, Bank Permata perlu untuk mencantumkan layanan sarana kontak email pada postingan *twit* nya, karena *email* dapat membantu nasabah untuk mengirim dokumen dengan jumlah banyak atau bahkan sekedar memberikan laporan keluhan kepada bank. (3) Perlu bagi BNI untuk memberikan sosialisasi dalam bentuk gambar poster atau video yang memuat informasi lengkap mengenai pencegahan modus *social engineering*, agar dapat menarik minat nasabah dalam membaca.

SIMPULAN

Modus *social engineering* menyerang manusia dengan cara mengeksploitasi kelemahan atau dengan mengelabui korbannya, sehingga diperlukan kesadaran dari manusia itu sendiri untuk memahami ciri-ciri modus *social engineering* dan langkah-langkah pencegahannya. Dengan demikian, posisi bank-bank di Indonesia sebagai elemen *controller* memiliki peran penting untuk mengatasi serangan *social engineering* yang dialami oleh nasabah bank, yaitu dengan memberikan sosialisasi mengenai pencegahan modus *social engineering* pada nasabah bank melalui media online yaitu media website dan media sosial twitter. Pemberian sosialisasi ini dapat mengurangi unsur *gullibility* pada nasabah, karena dapat memperkuat cara berfikir (*cognition*) nasabah dengan bertambahnya pengetahuan mengenai modus *social engineering* dan nasabah tidak mudah terjebak dalam unsur *situation* yang telah di rancangan oleh pelaku. Optimalisasi sosialisasi melalui website dan twitter dapat dilakukan dengan cara membuat konten yang memuat informasi secara lengkap dan terkini mengenai ciri-ciri modus *social engineering*, sarana layanan kontak, dan langkah-langkah pencegahan yang dapat divisualisasikan dalam bentuk video atau gambar poster yang di desain dengan menarik agar nasabah minat dalam membaca.

DAFTAR REFERENSI

Ali, L. (2019). Cyber crimes a constant threat for business sectors and its growth (a study of the online banking sectors in gcc). *The Journal of Developing Areas*, *53*.

Anderson, K. (2011). *Consumer fraud in the united states, 2011 the third ftc survey* (3rd ed.). Washington D.C.: Fededal Trade Commission.

Badan Siber dan Sandi Negara. (2020). *Rekap serangan siber (januari-april 2020)*. Diakses melalui https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Balzer, C., Oktavian, R., Zandi, M., Fairen-Jimenez, D., & Moghadam, P. Z. (2020). Wiz: A web-based tool for interactive visualization of big data. *Patterns*, *1*(8)

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*(2021), 656–661.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588.

Eck, J. (2003). Police problems: The complexity of problem theory, research and evaluation. *Crime Prevention Studies*, *15*, 79–113.

Gibbs, T. (2020). Seeking economic cyber security: A middle eastern example. *Journal of Money Laundering Control*, *23*(2), 493–507.

Greenspan, S. (2008). *Annal of gullibility: Why we get duped and how to avoid it: Why we get duped and how to avoid it*. Santa Barbara, CA: ABC-CLIO.

Hasan, A., & Febriany, L. (2021). Identifikasi tindakan pengawasan dan pencegahan terhadap kejahatan finansial perbankan syariah selama masa pandemi covid 19. *Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(4), 1089–1090.

Hasugian, P. S. (2018). Perancangan website sebagai media promosi dan informasi. *Journal of Informatic Pelita Nusantara*, *3*.

Iryanti, Y. S., & Rahman, M. A. (2019). Promosi perpustakaan melalui media sosial twitter di perpustakaan

hukum daniel s. Lev. *Edulib*, *9*(2), 128–143.

Kävrestad, J. (2018). *Fundamentals of digital forensics. In fundamentals of digital forensics (second)*. Springer Nature Switzerland AG.

Miles, M. B., & Huberman, A. M. (1994). *An expanded sourcebook: Qualitative data analysis second edition*. London: Sage Publications.

Saunders, Lewis, & Thornhill. (2012). Research methods for business students. *In International Journal of the History of Sport. 30(1)*.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies. 12*. 133-151.

Tracy, S. J. . (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (1st ed.). John Wiley & Sons, Ltd.,.

We are social. (2022). *Indonesian digital report 2022. In we are social (p. 113)*. Diakses melalui https://datareportal.com/reports/digital-2021-indonesia