e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 17 Mei 2023, Revised: 3 Juni 2023, Publish: 4 Juni 2023

JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking

Adi Wibowo Noor Fikri[1], Achmad Fauzi[2], Aldi Alfathur Rachman[3], Anggita Khaerunisa[4], Dhea Puspita Sari[5], Puput Vernanda[6], Raudhatul Hikmah[7], Tiara Putri Fadyanti[8]

[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, adi.noor@dsn.ubharajaya.ac.id
[2.] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Universitas Bhayangkara Jakarta Raya, Indonesia, raudhatulhikmah29@gmail.com
[4.] Universitas Bhayangkara Jakarta Raya, Indonesia, dheapuspitasari972@gmail.com
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, vernanda472@gmail.com
[6.] Universitas Bhayangkara Jakarta Raya, Indonesia, aldialfathur17@gmail.com
[7.] Universitas Bhayangkara Jakarta Raya, Indonesia, anggitanisa37@gmail.com
[8.] Universitas Bhayangkara Jakarta Raya, Indonesia, tiarafadyanti@gmail.com

Corresponding Author: Adi Wibowo Noor Fikri

Abstract: *The purpose of this study is to find out the types of phishing, and how phishing works so that data theft occurs in the banking world. Quantitative methods are used to find answers to research questions by looking for studies related to phishing threats in online banking services and carrying out a narrative synthesis of these findings. The lack of user knowledge and the psychological privacy of users of social networking services users are considered to be factors that cause phishing. Effective prevention of phishing threats can be achieved by educating users about cybercrime threats, prevention at the email level, using anti-phishing software, and implementing one-time password systems in banking services. Users are required to have good knowledge about the threat of crime, especially phishing, and the Bank has the responsibility to educate on threats that have the potential to harm users.*

Keyword: *Phishing, Security, Banking, Social Networks.*

Abstrak: Tujuan dari penelitian ini adalah untuk mengetahui jenis-jenis phishing, dan cara kerja phishing sehingga terjadi pencurian data di dunia perbankan. Metode kuantitatif digunakan untuk mencari jawaban atas pertanyaan penelitian dengan mencari kajian terkait ancaman phishing pada layanan perbankan online dan melakukan sintesa naratif dari temuan tersebut. Kurangnya pengetahuan pengguna dan privasi psikologis pengguna layanan jejaring sosial dianggap sebagai faktor penyebab phishing. Pencegahan ancaman phishing yang efektif dapat dicapai dengan mendidik pengguna tentang ancaman kejahatan dunia maya,

pencegahan di tingkat email, menggunakan perangkat lunak anti-phishing, dan menerapkan sistem kata sandi satu kali dalam layanan perbankan. Pengguna wajib memiliki pengetahuan yang baik tentang ancaman kejahatan, khususnya phishing, dan Bank memiliki tanggung jawab untuk mengedukasi ancaman yang berpotensi merugikan Pengguna.

Kata Kunci: Phishing, Keamanan, Perbankan, Jejaring Sosial.

PENDAHULUAN

Perkembangan Teknologi informasi dan Komunikasi (ICT) di dunia sangat terasa fungsinya pada beragam sektor Industri, Perbankan ataupun usaha kecil-Menengah (UKM). Manfaat efisiensi dan efektivitasnya dirasakan oleh berbagai sektor tersebut pada sisi operasional ataupun peningkatan layanan untuk penggunanya.

Tetapi perkembangan ini menimbulkan tantangan baru melalui kemunculan beraneka ragam tindak kriminal berbasis siber (*cyber crime*) dari berbagai pihak yang berupaya melakukan eksploitasi kelemahan sistem serta pencerahan pengguna terhadap Sistem informasi. Bentuk *cyber crime* yang para *fraudster* lakukan salah satunya yaitu *Phishing* (Radiansyah, Candiawan, et al., 2016)

Banyak hal dan informasi yang harus dilindungi terhadap teks melalui e-mail maupun SMS. Dalam keamanan informasi seperti kerahasiaan data-data penting, integritas informasi serta keberadaan informasi yang akurat. Kesadaran atas keamanan informasi juga meliputi pada penggunaan program yang aman serta perilaku positif yang mengutamakan keamanan guna mencegah terjadinya *phishing* di sekitar kita (Vadila & Pratama, 2021).

Sehubungan dengan pentingnya kesadaran akan ancaman Phishing, peneliti akan melakukan analisis pada kesadaran masyarakat pengguna internet Indonesia. Penelitian ini akan membahas bagaimana kesadaran ancaman Phishing pada setiap nasabah. Dengan adanya penelitian ini diharapkan menjadi informasi terhadap tingkat kesadaran ancaman Phishing pada masyarakat Indonesia.

Salah satu upaya untuk mengantisipasi serangan phishing adalah dengan cara tidak mengklik link atau tautan sembarangan menggunakan akun sosial media pribadi apabila terdapat link yang masuk melalui akun media sosial yang tidak dikenal patut dicurigai termasuk jebakan phishing pada akun sosial media yang ingin membagikan hal-hal buruk untuk pengguna media sosial lainnya.

1. Jelaskan apa saja jenis penipuan *phishing* dan cara kerjanya yang biasanya sering terjadi di dunia perbankan?
2. Apa penyebab dan pencegahan *phising* pada *online* banking?
3. Jelaskan peristiwa yang terkait pada bank BCA dengan permasalahan *phishing*?

METODE

Metode penelitian merupakan cara yang dipakai dalam pemecahan masalah yang akan diteliti pada saat penelitian terjadi. Ketika artikel ini ditulis, peneliti memakai metode penelitian kualitatif. Penelitian kualitatif merupakan penelitian yang menekankan pada kualitas ataupun hal terpenting dalam sifat sebuah barang ataupun objek yang dapat berbentuk peristiwa, fenomena, ataupun gejala sosial. Peristiwa tersebut memiliki arti yang bisa menjadi pelajaran berharga guna mengembangkan konsep teoritis.

Jenis penelitian kualitatif yang dipakai yaitu penelitian deskriptif dengan metode kepustakaan. Kritik sastra adalah metode penelitian dimana masalah yang diteliti akan diperiksa serta dipertimbangkan secara kritis. Peneliti akan memakai sumber data sekunder yang didapatkan melalui dokumen, arsip, buku, makalah, serta hasil penelitian yang sudah ada. Milles dan Huberman (1984) dalam Muftiadi et al. (2022) mengungkapkan bahwa dalam

melakukan analisis data, peneliti harus melakukan beberapa langkah diantaranyaa reduksi data, penyajian data, serta inferensi atau validasi. Maka dari itu pada artikel mengenai analisis keamanan sistem operasi dalam menghadapi ancaman phishing dalam layanan online banking akan menganalisis lebih lanjut tentang permasalahan yang terjadi.

Tabel 1: Hasil Penelitian yang Relevan Terdahulu

No	Author, Tahun	Hasil Riset	Persamaan dengan Riset	Perbedaan dengan Riset
1	Aseh Ginanjar, dkk, 2018	Penegakan hukum pidana serangan phishing pada layanan online banking	Keamanan layanan online sama-sama pengancaman dari phishing	Tidak ada data respon dari DNS query paket data nomor pada jurnal yang dikerjakan
2	Mia Haryati Wibowo Dan Nur Fatimah 2017	Hasil riset menyatakan penulis penyampaian pesan agar masyarakat harus mengetahui hal-hal yang mencurigakan pada akun jejaring sosial ataupun situs lainnya.	Menjelaskan cara-cara mencegah ataupun mengantisipasi serangan phishing melalui website berdasarkan berbagai literatur	Tidak ada
3	Koko Canigo, Tata Sutobri, 2023	Hasil riset mengungkapkan terdapat beberapa langkah yang harus dilakukan peneliti dalam melakukan analisis.	Sama-sama melakukan analisis data antara lain redukasi data, display data, dan inferensi atau validasi.	Tidak ada
4	Firda Atsalis Maulidya Hasanah, 2019	Hasil riset menyatakan yaitu faktor mayoritas memiliki kurangnya pengetahuan yang baik mengenai ancaman phising sehingga dimanfaatkan phisher untuk mendapatkan data-data sensitif.	Phising memiliki tujuan untuk menjebak korban yang dilakukan oleh penjebak (phisher).	Tidak ada
5	Windy Ratna Yulifa, 2012	Hasil riset ini menyatakan tindakan penipuan yang menggunakan email palsu.	Sama-sama menggunakan email palsu untuk mendapatkan data tersebut.	Tidak ada
6	Amin Muftiadi, dkk, 2022	Hasil riset menyatakan bahwa penyebab kejadian phishing pada layanan online banking yaitu kurangnya pengetahuan pengguna, psikologi serta privasi layanan jaringan sosial.	Persamaan pada riset ini sama-sama membahas terkait phishing yang terjadi pada layanan online banking perbankan.	Tidak ada
7	Ikhsan Radiansyah, dkk, 2014	Hasil riset menyatakan bahwa kasus penipuan online pada layanan online bangking bukan hanya dipegang oleh pihak bank saja tetapi pihak pengguna ikut bertanggung jawab atas	Persamaan pada riset ini membahas tentang phising dengan meretas akun bangking melalui pencurian informasi melalui gmail .	Tidak ada

		terjadinya kasus tersebut.		
8	Anisa Gustiani, 2019	Hasil riset menjelaskan tentang ancaman serangan phising saat memakai layanan online bangking dan kurangnya pengetahuan privasi social networking services .	Persamaannya sama sama membahas persoalan phising pada layanan online bangking.	Tidak ada
9	Nunu Vadila Ahmad R. Pratama, 2021	Hasil riset menemukan kasus penipuan online dengan cara memanipulasi untuk menipu korban dan kesadaran pengguna terhadap informasi tentang kerahasiaan password .	Persamaannya yaitu menginformasikan tentang phising dan juga ancamannya	Tidak ada
10	Amin Muftiadi , dkk, 2022	Hasil riset menyatakan bahwa penyebab terjadinya phising dan layanan online bangking adalah minimnya pengetahuan pengguna, dengan demikian pencegahan serangan phising pada layanan online bangking dapat dilakukan melalui edukasi pengguna, pencegahan phising di level email, penggunaan software anati phising, penggunaan sistem OTP pada sistem perbankan	Persamaan pada riset yaitu membahas terkait phising yang terjadi pada layanan online bangking perbankan .	Tidak ada

HASIL DAN PEMBAHASAN

Jenis-Jenis Dan Cara Kerja *Phishing*

1. Spear Phishing

Spear phishing dilaksanakan melalui pengiriman email kepada target korban dengan menyamar sebagai pengirim yang dipercaya. Isi emailnya yaitu link yang memandu target membuka website palsu yang dipenuhi malware, atau biasa dikenal sebagai phishing site. Phishing site merupakan upaya penipuan guna mengelabui korbannya dengan memakai web ataupun situs palsu. Hal ini bertujuan supaya phiser dapat melakukan pencurian informasi sensitif berupa kredensial akun ataupun informasi keuangan milik korban.

Cara kerja serupa ketika penangkapan ikan yang ditargetkan dengan tombak (*spear*). Teknik phising ini juga menyasar korban yang telah ditargetkan pelaku pencuri data (*phisher*). Maknanya, phisher telah mempunyai suatu tujuan serta informasi yang diperlukan dalam menghubungi korbannya melalui email, pesan WhatsApp, SMS, telepon, dan lain-lain. Dibandingkan dengan teknik lain, tingkat keberhasilan *spear phishing* lebih besar sebab dibuat untuk lebih meyakinkan target korban. Namun tidak perlu ditakutkan

sebab pesan phishing dapat ditemukan melalui kesalahan dalam pemakaian tata bahasa ataupun tanda bacanya.

2. Deceptive Phising

   Deceptive phising merupakan usaha menipu melalui penggunaan identitas instansi, perusahaan, ataupun pihak-pihak tertentu yang berpeluang besar dikenal. Cara kerjanya yaitu pelaku phishing memakai alamat email beserta link yang mirip dengan instansi, perusahaan ataupun merek terkenal. Teknik ini bisa dicoba melalui email, pesan teks, ataupun melalui WhatsApp yang sedang ramai terjadi.

3. Web Phishing

   Situs web yang dibuat dengan maksud melaksanakan penipuan yang mencoba memperoleh informasi sensitive seperti nomor kartu kredit, password, ataupun informasi penting lain. Pada umumnya web phishing memiliki bentuk yang serupa dengan website aslinya, dari tampilannya ataupun nama domain yang bertujuan membuat rasa curiga calon korbannya seminimal mungkin. Secara umum berdasarkan definisi tersebut, kesimpulan yang dapat diambil yaitu web phishing merupakan suatu situs web biasa yang dibuat sengaja dengan tujuan untuk kejahatan. Web phising di Indonesia umumnya memiliki tujuan untuk pengambilalihan akun media sosial seseorang. Sedangkan di luar negeri, kasus ini dapat lebih buruk lagi sebab melibatkan kredensial akses seperti kartu kredit serta rekening bank online pribadi.

   Web phishing sebenarnya bekerja dengan cara yang cukup sederhana, yaitu phisher menargetkan situs web yang dipercay adengan baik serta terkenal di masyarakat. Contohnya yaitu facebook.com, twitter.com, instagram.com, gmail.com, ataupun situs pembayaran seperti paypal, gopay, LinkAja yang saat ini sedang populer. Biasanya jika pelaku sudah menemukan target yang ingin dituju, pelaku langsung membuat website palsu atau web phising yang bentuk serta nama domainnya dimiripkan dengan website asli.

   Contoh-contoh web phishing yang pernah ditemui yaitu fatebook.com (*salinan facebook.com*), kikbca.com (*salinan klikbca.com*), twltter.com (*salinan Twitter.com, dimana ada penggantian huruf "i" menjadi "L"*). Saat menggunakan nama domain serta tampilannya yang serupa, web phishing mencoba mengelabui pengguna agar login dengan informasi yang benar. Informasi yang dimasukkan tersebut selanjutnya disimpan dalam database secara otomatis supaya pelaku penyebar web phising dapat mengakses akun pengguna di situs web resminya. Biasanya akun media sosial yang terjebak phishing mempunyai tanda-tanda sering membuat posingan tautan yang memuat hal aneh, status yang tidak biasa, ataupun dapat pula dimanfaatkan dalam menjalankan modus penipuan yang direncanakan.

Apa Penyebab Dan Pencegahan Phising Pada Online Banking?

Faktor yang menyebabkan kemunculan ancaman serangan *phishing* dalam layanan online banking yaitu kurangnya pengetahuan masyarakat pada seberapa penting untuk menjaga keamanan datanya. Dhamija, Tygar, & Hearst (2006) dalam Hasanah (2014) menyatakan pengguna diduga tidak mempunyai pengetahuan yang memadai tentang sistem komputer khususnya ketika melihat perbedaan domain resmi dengan palsu. Pernyataan tersebut diperkuat oleh Mohammad, Thabtah, & McCluskey (2015) dalam Hasanah (2014) yang juga menyatakan faktor yang membuat seseorang menjadi korban serangan *phishing* yaitu sebagian korbannya mempunyai pengetahuan yang kurang atas ancaman perbuatan kriminal online beserta ancaman phishing, tidak mempunyai strategi yang baik untuk mengetahui tanda-tanda serangan phishing, lebih fokus pada kontennya daripada indikator dalam websitenya, serta tidak memahami prosedur layanan online yang digunakan yang berujung terperangkap saat memperoleh email dari layanan online yang digunakan mengenai

informasi pemeliharaan atau informasi lain yang dimanfaatkan phisher guna memperoleh data pribadi penggunanya. Faktor lainnya yang menjadikan penggunanya bisa terperangkap dalam serangan phising yaitu sifat naif dalam memakai layanan online banking. Biasanya ada kesamaan kata sandi yang akan digunakan oleh pengguna untuk beberapa halaman website, dimana password tersebut tidak jauh dari informasi umum seperti nama anak, tanggal lahir, atau nama hewan yang dirawat.

Phishing bisa dicegah dengan memasang filter pada email yang membagi email menjadi dua kategori yakni asli dan palsu. Dalam pemakaiannya, perusahaan bisa membuat perlindunagn bagi karyawan serta pelanggannya dari email spam yang bisa memicu ancaman pencurian data. Cara lain untuk mencegah *phishing* juga bisa memakai perangkat lunak anti-phishing selain indikator keamanan pada browser, contohnya menggunakan protokol HTTPS (SSL certifed) pada situs. AntiPhish memiliki tujuan dalam perlindungan penggunanya dari halaman situs palsu dengan menyajikan pesan waspada saat pengguna ingin menginput data sensitif (username, kata sandi) pada halaman yang tidak kredibel. GoldPhish juga bisa digunakan, yaitu suatu plugin yang terpasang pada browser sebagai perlindungan dari zero-day phishing sites. Umumnya phishing dicegah melalui penggunaan teknik blacklist ataupun whitelist atas URL phishing yang sudah terdeteksi. GoldPhish dianggap akurat untuk pendeteksian 100% website asli serta 98% website phishing (Dunlop, et al., 2010 dalam Hasanah, 2014)

Pihak perbankan mencegah ancaman pishing melalui penggunaan sistem One Time Password (OTP) yang merupakan sistem autentikasi dengan pengiriman password melalui pesan teks oleh institusi perbankan kepada penggunanya, tetapi password ini hanya bisa dipakai satu kali. IT Security Manager salah satu bank di Indonesia telah menyatakan pihak perbankan sudah melaksanakan tindakan untuk mencegah serangan *phishing* berdasarkan tiga aspek yaitu menusia, proses, dan teknologi. Ditambahkan pula bahwa layanan online banking di Indonesia sudah memberikan peringatan kepada penggunanya melalui pemasangan pesan waspada. Sebagaimana Bank Mandiri yang melakukan pemasangan pesan waspada yang berbunyi "Hentikan transaksi jika anda diminta sinkronisasi token pada saat login dan pastikan komputer anda bersih dari virus". Selain itu Bank BCA juga menggunakan pesan "Waspada virus trojan, malware dan spyware. Stop! Jika anda menemukan hal yang tidak biasa pada saat bertransaksi Internet Banking, Stop jangan dilanjutkan!" sebagai tanda peringatan kewaspadaan (Aktorian, 2015 dalam Hasanah (2014). Tetapi pada akhirnya tergantung pada tingkat kesadaran para pengguna apakah terhadap pesan waspada yang diberikan.

Kasus Peristiwa Bank BCA Dengan *Phishing*

Kasus pembobolan internet banking bank BCA terjadi pada tahun 2001 oleh Steven Haryanto yang merupakan mantan mahasiswa ITB Bandung serta pegawai media internet (*satunet.com*) menurut Muftiadi et al. (2022). Padahal diketahui Steven merupakan seorang insinyur kimia, bukan insinyur listrik ataupun komputer. Gagasan tersebut muncul saat Stephen mengetikkan alamat situs web. Lalu Steven membeli domain internet dengan harga sekitar $20 memakai nama dengan kesalahan pengetikan serta nampak serupa dengan situs internet banking BCA. Contoh kesalahan pengetikan tersebut yaitu *http://www.klikbca.com, misalnya: wwwklikbca.com, kilkbca. .com, klikbca.com, klikbca.com, klikbac.com.*

Penampilan pada situs tersebut dibuat semirip mungkin dengan situs resninya sehingga Nasabah Bank tidak menyadari bahwa mereka mengakses situs palsu. Steven bisa mendapatkan ID pengguna beserta kata sandi dari pengguna yang masuk ke perangkat lunak, namun dia tidak mencoba tindakan kriminal seperti pencurian uang pengguna, hal tersebut tidak ada maksud tertentu karena hanya penasaran dengan seberapa banyak pengguna yang tidak mengetahui pemakaian *klikbca.com* dan menguji tingkat keamanan situs.

Steven Haryanto dapat disebut hacker sebab tindakannya merupakan peretasan sistem pengguna lain dengann privasi yang terlindungi. Tindakan tersebut dikenal sebagai hacking. Steven bisa dikategorikan sebagai tipe hacker campuran dari white hat hacker dengan black hat hacker dimana dia hanya melakukan percobaan guna melihat tingkat keamanan situs internet banking Bank BCA. Maksud white hat hacker yaitu tidak adanya tindakan pencurian uang pada nasabahnya, namun sekadar memperoleh ID pengguna serta kata sandi nasabah yang masuk ke situs internet banking palsu. Tetapi tindakan yang Steven lakukan juga termasuk hacker black hat yang menciptakan situs palsu yang tanpa diketahui memperoleh data orang lain. Steven merupakan pemindai, sniffer, dan cracker kata sandi.

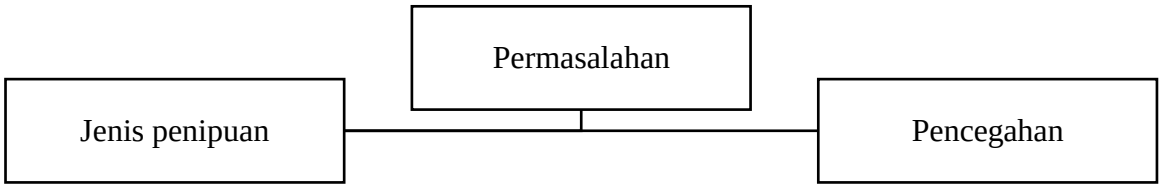
Skenario

Situs palsu dikirimkan oleh pelaku dari email dengan teks yang serupa dengan situs resminya, apabila target korban tidak teliti maka dia akan membuka situs palsu tersebut sesuai petunjuknya, termasuk memperbaharui akun guna memperoleh informasi lebih lanjut tentang data pribadinya. Korban akan dibawa menuju situs palsu yang telah di klik, kemudian penyerang bisa bertindak apapun menggunakan informasi tersebut, termasuk melakukan pencurian dana.

Dampak Phishing bank BCA

Kejadian tersebut berakibat pada nasabah serta bank yang menderita rugi, sebab informasi pribadi yang mencakup akses login situs web berpeluang terjadi pada nasabah lainnya. Pelaku tidak memperoleh keuntungan materi dari ini, sedangkan bank akan mendapatkan penurunan tingkat kepercayaan dari nasabahnya. Kasus ini bisa termasuk dalam Pasal 378 KUHP untuk tindak pidana penipuan mendapatkan informasi pribadi (*phishing*) melalui pengiriman email, karena Undang-Undang Nomor 11.

Kerangka Berpikir/ *Concept Framework*



Jenis penipuan

1. Spears phising dengan melalui pengiiriman e-mail terhadap target korban dengan menyamar sebagai pengirim yang dipercaya.
2. Deceptive phising dengan memlalui penggunaan identitas instansi, perusahaan, atau pihak-pihak tertentu yang berpeluang besar dikenal.
3. Web phising dengan melalui penipuan yang mencoba memperoleh informasi sensistif seperti nomor kartu kredit, password, atau informasi yang penting lainnya.

Permasalahan

Masyarakat mempunyai pengetahuan yang kurang atas ancaman perbuatan kriminal online beserta ancaman phising, lalu tidak mengetahui tanda-tanda serangan phising. Serta tidak memahami prosedur layanan online yang digunakan dan berujung terperangkap saat memperoleh email dari layanan online yang digunakan, sehingga phiser memanfaatkannya untuk memperoleh data pribadi para pengguna layanan online banking.

Pencegahan

1. Periksa URL situs web bank, pastikan pengguna mengunjungi situs web resmi bank.
2. Jangan membagikan informasi pribadi seperti nomor rekening, password, dan NIK KTP atau email melalui email atau pesan teks dari sumber yang tidak dikenal.
3. Hindari mengklik tautan di E-mail, pesan teks dari sumber yang tidak dikenal.
4. Jangan memasukan data pribadi dihalaman web yang mencurigakan, sebelumnya periksa terlebih dahulu kebenaran alamat web sebelum memasukan data pribadi.
5. Gunakan aplikasi keamanan seperti Anti-Virus dan Anti-Malware untuk melindungi perangkat dari kemungkinan adware, spyware, atau perangkat lunak jahat lainnya.

KESIMPULAN

Phishing adalah sebuah bentuk kegiatan yang memiliki sifat pengancaman atau penjebakan seseorang melalui rencana untuk memancing calon korban dengan menipunya sehingga secara tidak langsung membagikan seluruh informasi yang diperlukan oleh pelaku. Ancaman phishing berasal dari berbagai sumber antara lain email, website, serta malware. Menurut hasil survey yang sudah dilaksanakan, website menjadi sumber ancaman phishing terbanyak serta tindakan untuk mencegah yang sering dilaksanakan yaitu *self-efficacy* (keyakinan seseorang dalam mengambil sebuah tindakan).

Berdasarkan kasus-kasus yang terjadi, Phishing pada kasus bank BCA sering terjadi dan pelaku kejahatan dapat berhasil mengambil alih akun bank korban tersebut. Maka dari itu, Para pengguna sangat penting dihimbau selalu waspada terhadap E-mail, SMS. Atau Telepon yang mencurigakan yang meminta informasi sensitif seperti Nomer Rekening atau Kata Sandi. Beberapa Tindakan pencegahan yang dapat dilakukan adalah memeriksa keaslian sumber informasi dan memastikan bahwa situs yang dikunjungi adalah situs resmi Bank.

REFERENSI

Caniago, K., Sutabri, T., Magister, S., Informatika, T., Darma, U. B., & Darma, U. B. (2023). *Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau*. *8*, 117–125.

Ginanjar, A., Widiyasono, N., & Gunawan, R. (2018). *Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process*. *2*, 147–157. https://doi.org/10.21460/jutei.2018.22.103

Gustiani, A. (2019). *ANALISIS ANCAMAN PHISING TERHADAP LAYANAN ONLINE BANKING*. *1643500141*.

Hasanah, F. A. M. (2014). *Ancaman phising pada pengguna online banking*.

Muftiadi, A., Putri, T., Agustina, M., & Evi, M. (2022). *Studi kasus keamanan jaringan komputer : analisis ancaman phising terhadap layanan online banking*. *1*(2), 60–65.

Radiansyah, I., Candiawan, & Priyadi, Y. (2016). *ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING*. *7*(1).

Radiansyah, I., Candiwan, & Priyadi, Y. (2016). *ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING ANALYZE PHISING THREATS IN ONLINE*.

Vadila, N., & Pratama, A. R. (2021). *Analisis Kesadaran Keamanan Terhadap Ancaman Phishing*.

Wibowo, M. H., & Fatimah, N. (2017). *Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime*. *1*, 1–5.

Yulifa, W. R. (2021). *PENEGAKAN HUKUM PIDANA SERANGAN PHISING PADA LAYANAN ONLINE BANKING*.