ANALISIS ANCAMAN PHISHING DALAM LAYANAN *E-COMMERCE*

Irvan Hadi Ramadhan[1], Erna Kumalasari Nurnawati[2]
Institut Sains dan Teknologi AKPRIND Yogyakarta
e-mail : [1]hadiivan40@gmail.com, [2]ernakumala@akprind.ac.id

ABSTRACT

Phishing is a threat that uses social engineering techniques and deceives users by impersonating an authorized person, being a seller, or being a party to e-commerce itself with the intent and purpose of obtaining sensitive user data. This study discusses the factors that cause the emergence of phishing and prevent the threat of phishing attacks. The method used in this study is the Literature Review method. The Literature Review method is used to find answers to research questions by looking for studies related to the research topic (Analysis of Phishing Threats in E-Commerce Services) and performing narrative synthesis on these findings. This study's results indicate a lack of knowledge on users, psychology, and privacy of social network services. Thus, the prevention of phishing attacks on e-commerce services is carried out. Prevention is to provide education to users, so users who have received education will easily detect and avoid phishing threats contained in e-mails and URLs or websites. Preventing phishing attacks at the e-mail level, using anti-phishing applications (software), and using a verification code system (OTP) to protect the security of information and user accounts. Users must have good knowledge of the threats of phishing crimes and e-commerce parties must provide information and are responsible for providing education about threats that can harm users.

Keywords : *E-commerce, E-mail, Phishing, Website*

INTISARI

Phishing merupakan ancaman yang menggunakan teknik rekayasa sosial dan mengelabui pengguna dengan cara menyamar sebagai orang yang berwenang, menjadi penjual ataupun menjadi pihak dari e-commerce itu sendiri dengan maksud dan tujuan untuk mendapatkan data-data sensitif pengguna. Penelitian ini membahas faktor-faktor penyebab munculnya phishing serta melakukan pencegahan terhadap ancaman serangan phishing. Metode yang digunakan dalam penelitian ini adalah metode Literature Review. Metode Literature Review digunakan untuk menemukan jawaban atas pertanyaan-pertanyaan penelitian dengan mencari studi-studi yang berkaitan dengan topik penelitian (Analisis Ancaman Phishing Dalam Layanan E-Commerce) dan melakukan narrative synthesis pada temuan tersebut. Hasil dari penelitian ini menunjukkan bahwa minimnya pengetahuan pada pengguna, psikologis serta privasi social network service. Dengan demikian dilakukanlah pencegahan serangan phishing pada layanan e-commerce. Pencegahan yang dilakukan adalah memberikan edukasi kepada pengguna, dengan demikian pengguna yang telah mendapatkan edukasi akan dengan mudah mendeteksi dan menghindari ancaman phishing yang terdapat pada e-mail dan URL atau situs web. Melakukan pencegahan serangan phishing di level e-mail, menggunakan aplikasi (software) anti-phishing, serta menggunakan sistem kode verifikasi (OTP) untuk melindungi keamanan informasi dan akun pengguna. Pengguna harus memiliki pengetahuan yang baik dalam mengenai acaman kejahatan phishing serta pihak e-commerce harus memberikan informasi dan tanggung jawab untuk memberikan edukasi terhadap ancaman yang dapat merugikan pengguna.

Kata kunci : *E-commerce, E-mail, Phishing, Website*

1. PENDAHULUAN

Di era teknologi informasi dan komunikasi saat ini segala sesuatu dapat dilakukan dengan mudah dan cepat. Hampir seluruh aspek dalam kehidupan tidak lepas dengan yang namanya teknologi informasi dan komunikasi. Hal ini dikarenakan adanya teknologi internet yang memudahkan manusia dalam melakukan pertukaran informasi dan komukasi jarak jauh dengan cepat. Dengan adanya teknologi internet saat ini dapat mempermudah pengguna dalam mengakses *website* ataupun *web apps* sehingga pengguna dapat melakukan aktivitas salah satunya adalah melakukan transaksi jual beli *online* (*e-commerce*).

Penggunaan *website e-commerce* untuk transaksi secara online saat ini sudah menjadi kebutuhan pokok masyarakat di Indonesia, hal ini didukung oleh Pratama Afrianto & Irwansyah (2021) yang menyatakan bahwa saat ini belanja online sudah menjadi gaya hidup di tengah masyarakat Indonesia. Menurut Hadya Jayani, (2021) tingkat penjualan *e-commerce* pada 2021 sebesar US$53 miliar, hal ini diakibatkan karena teknologi informasi mampu menyediakan peluang bagi penjual untuk menjangkau pembeli secara lebih luas.

Layanan *e-commerce* memberikan manfaat bagi penjual maupun pembeli, namun disisi lain terdapat dampak negatif penggunaan layanan tersebut. Salah satu penyalahgunaan layanan *e-commerce* dalam teknologi internet adalah phishing Menurut Ginanjar et al. (2018) kejahatan phishing dapat dilakukan menggunakan teknik rekayasa website yang mengakibatkan kerugian finasial, pencurian identitas seseorang dan pembobolan akun. Menurut Indonesia Anti-Phishing Data Exchange (IDADX) jumlah kejahatan phishing di Indonesia tahun 2022 dalam kuartal pertama mencapai 3.180 laporan phishing, sedangkan pada kuartal kedua 2022 mengalami kenaikan menjadi 5.579 laporan, angka tersebut menunjukan bahwa pelaku phishing di Indonesia saat ini semakin meningkat. Sektor *e-commerce* menjadi salah satu target kejahatan phishing ke dua terbesar yaitu mencapai 32% setelah lembaga keuangan yang mencapai 41% pada kuartal kedua pada tahun 2022, hal tersebut membuktikan bahwa kejahatan phishing pada sektor *e-commerce* di *Indonesia* cukup tinggi.

Table 1. Sektor Incaran Phishing di Indonesia Kuartal II

Sektor	Jumlah Laporan Phishing	Persentase
Lembaga Keuangan	2.287	41%
E-Commerce/Retail	1.785	32%
Media Sosial	1.171	21%
Cryptocurrency	168	3%
Gaming	168	3%
ISP	0	0%
Malware	0	0%

Sumber: IDADX, 2022

Phishing merupakan upaya untuk mendapatkan informasi sensitif pengguna melalui *e-mail* atau situs web palsu dengan cara meniru tampilan situs web yang asli atau resmi. Pelaku menggunakan *e-mail,* spanduk, atau pop-up ntuk megelabui pengguna agar mengarahkannya ke situs web palsu dan meminta mereka memberikan informasi pribadi. Pada saat inilah pelaku memanfatkan ketidakpedulian pengguna untuk mendapatkan informasi pribadi.

Phishing bekerja dengan cara memanipulasi tautan sehingga terlihat mirip dengan alamat situs asli. Trik yang umum digunakan pelaku phishing adalah menggunakan subdomain palsu dan *borken* URL, contohnya adalah URL www.shopee.co.id diubah menjadi www.shopee.net atau www.shopee.comwww.shopee.com. Pelaku akan membujuk pengguna untuk mengungkapkan informasi pribadinya melalui situs palsu yang menyerupai situs asli melalui *e-mail* yang pelaku kirim, halaman situs web dibuat semirip mungkin dengan situs resmi sehingga pengguna akan percaya dan memasukan data-data pribadinya.

Terdapat teknik yang di gunakan oleh pelaku phishing yaitu menggunakan metode *e-mail spoofing*, *e-mail* akan dikirim kepada jutaan pengguna dengan mengaku dari pihak institusi resmi, *e-mail* yang dikirim biasanya berisi permintaan nomor kredit, kata sandi, atau menyuruh pengguna untuk mengunduh formulir tertentu. Metode yang dilakukan phishing selajutnya adalah *Internet Submision, Internet Submision* merupakan metode yang paling canggih, pelaku phishing akan berada di tengah antara situs web resmi dengan sistem phishing. Metode selanjutnya adalah menggunakan teknik pesan instan, di mana pelaku akan mengirim pesan berisikan tautan yang akan mengarahkan pengguna pada situs palsu yang menyerupai situs resmi. Kejahatan phishing menggunakan metode *host* trojan dengan cara meretas lalu masuk kedalam akun pengguna untuk mengumpulkan kredensial melalui komputer pengguna, lalu informasi akan dikirim ke pelaku. Selanjutnya yaitu metode manipulasi tautan (Link) yaitu pelaku akan mengirimkan tautan ke sebuah situs web, pada saat pengguna mengklik tautan maka pengguna akan di arahakan ke situs web yang menyerupai situs resmi.

Kasus phishing di indonesia marak terjadi pada *e-commerce* seperti tokopedia, shopee, bukalapak dan sebagainya. Menurut Dara, (2021) pengguna *e-commerce* shopee mengalami kerugian hingga Rp 8.600.000 akibat kasus pencurian phishing. Modus yang dilakukan pelaku yaitu dengan melakukan panggilan, memberitahu bahwa korban mendapat hadiah, kemudian pelaku mengirimkan link kepada korban dan meminta memasukan kode *On-Time Password* (OTP) yang telah dikirim melalui SMS. Kasus lain terjadi pada pengguna e-commerce bukalapak dengan cara pelaku mengirimkan link asuransi palsu kepada korban yang sedang melakukan pembelian 1 unit sepeda, namun link yang pelaku kirim adalah link phishing, hal ini mengakibatkan pelaku berhasil masuk ke dalam akun bukalapak korban dan seketika setatus pembelian menjadi terkirim, sehingga dana korban langsung cair ke rekening pelaku (Dokubani, 2020).

Kasus phishing terhadap dunia *e-commerce* mendorong akademisi untuk melakukan penelitian mengenai deskripsi serangan phishing, tipe phishing dan pencegahan kejahatan phishing. Telah banyak studi penelitian terhadap serangan phishing pada sektor finansial. Dengan demikian, pada penelitian ini akan dilakukan analisis serangan phishing pada sektor e-commerce berdasarkan metode *literature review*. Dengan tujuan yaitu menganalisis faktor apa saja yang menyebabkan terjadinya phishing pada sektor *e-commerce* dan memberikan rekomendasi pencegahan terhadap ancaman phishing.

2. METODE PENELITIAN

Penulisan ini menggukanan metode analisis deskriptif kualitatif dengan pengumpulan data melalui kajian literature dan pengamatan website Mediakonsumen.com sebagai wadah pengaduan konsumen yang mengalami berbagai kendala termasuk penipuan online (phishing) pada layanan *e-commerce*. Pencarian referensi teori dan data yang telah dipublikasi menjadi salah satu rujukan dalam kegiatan penulisan ini. Menurut (Creswell, 2014) menyatakan bahwa kajian literature ringkasan mengenai sumber-sumber yang relevan untuk menyajikan teori serta informasi untuk diorganisasikan. Analisis deskriptif digunakan sebagai cara mendeskripsikan fenomena yang kemudian disusul dengan analisis, yang tidak hanya diuraikan namun juga memberikan pemahaman dan penjelasan secukupnya. Setiap fakta penelitian dibandingkan dan dicocokan satu sama lain. Apabila terdapat kesamaan antara penelitian A dan B, maka fakta/bukti temuan penelitian akan dijadikan landasan penelitian ini. Fakta/bukti yang dibutuhkan dalam penelitian ini adalah faktor-faktor yang menyebabkan phishing pada sektor *e-*

commerce.

3. HASIL DAN PEMBAHASAN

Phishing pada *e-commerce* merupakan ancaman menggunakan teknik rekayasa sosial dengan mengelabui pengguna. Pelaku mengelabui pengguna dengan mengaku sebagai penjual atau dari pihak e-commerce dan melakukan penawaran palsu melalui *e-mail*, pesan singkat dan panggilan telepon. Setelah mendapatkan data pribadi pengguna, selanjutnya pelaku menggunakan data korban untuk keuntungan pribadi.

3.1 Faktor penyebab munculnya ancaman phishing

Bab ini akan menjelaskan mengenai faktor penyebab munculnya phishing pada saat pengguna menggunakan aplikasi atau *website e-commerce* serta pencegahan terhadap ancaman tersebut. Berikut adalah tabel mengenain faktor penyebab terjadinya kejahatan phishing berdasarkan *study literature.*

Table 2. Faktor penyebab phishing berdasarkan *study literature*

No	Nama Penulis dan Tahun	Faktor penyebab phishing
1	(Mohammad et al., 2015)	Pengetahuan pengguna minim
2	(Volkamer et al., 2017)	Pengetahuan pengguna minim
3	(Muftiadi et al., 2022)	Pengetahuan pengguna minim
4	(Vishwanath et al., 2011)	Psikologi
5	(Radiansyah et al., 2016)	Pengetahuan pengguna minim, psikologis dan privasi *social networking services*
6	(Malik & Malik, 2011)	Privasi *social networking service*
7	(Gulo et al., 2021)	Pengetahuan pengguna minim
8	(Zielinska et al., 2015)	Pengetahuan pengguna minim
9	(Abroshan et al., 2018)	Psikologis
10	(Yang et al., 2022)	Pengetahuan pengguna minim
11	(Alsharnouby et al., 2015)	Pengetahuan pengguna minim
12	(Button et al., 2014)	Psikologis
13	(Hasanah, 2014)	Pengetahuan pengguna minim
14	(Arachchilage & Love, 2014)	Pengetahuan pengguna minim
15	(Khairunnisa, 2021)	Pngetahuan pengguna minim, psikologis dan privasi *social networking services*

Mohammad et al., (2015) mengungkapkan bahwa mayoritas pengguna tidak memiliki pengetahuan yang baik terhadap ancaman phishing, minimnya pengetahuan dan tidak memiliki setrategi yang baik dalam menangani ancaman serangan phishing, pengguna tidak mengetahui prosedur layanan online sehingga dapat dengan mudah terjebak penipuan melalui *e-mail*, penggilan telepon, atau pesan singkat yang di manfaatkan phisher agar mendapatkan data-data sensitif pengguna untuk keuntungan pribadi.

Penelitian yang dilakukan Volkamer et al., (2017) mengungkapkan alasan mengapa pengguna menjadi korban kejahatan phishing, yaitu ketidak sadaran pengguna terhadap URL palsu, hal tersebut dikarenaan URL adalah satu-satunya akses yang dapat diadalka. Pengguna tidak mengetahui URL mana yang dapat dipercaya. Terdapat tiga opsi yaitu, tertanam dalam email, ditampilkan pada tooltip atau pada bilah status. Pengguna cenderung tidak memiliki akses ke URL asli, hal tersebut dikarenakan URL dikaburkan pelaku untuk pengalihan atau penggunaan URL pendek. Pengguna tidak memeriksa URL dengan benar sebelum mengklik situs, hal ini karena faktor ketidak sengajaan atau kebiasaan pengguna. Pengguna tidak memiliki pengetahuan dalam membedakan URL asli dengan URL phishing.

Faktor pengetahuan dan kesadaran pengguna terhadap ancaman serangan phishing juga didukung oleh Muftiadi et al., (2022). Dalam artikel tersebut penulis meneliti mengenai pengetahuan pengguna untuk mengidentifikasi website phishing. Pengetahuan pengguna terhadap domain, link atau website palsu yang menyerupai aslinya sangat minim, sehingga pengguna tidak menyadari bahwa telah menggunakan situs palsu.

Vishwanath et al., (2011) menyatakan bahwa pengguna merupakan faktor utama penyebab terjadinya phishing. Terdapat empat alasan mengapa phishing terjadi pada pengguna. Pertama adalah semakin banyaknya *e-mail* yang di terima pengguna, semakin besar peluang untuk ditipu. Yang kedua adalah pengguna cenderung membuka *e-mail* dari orang yang mereka kenal. Pengguna yang memiliki hubungan dengan lebih dari satu lembaga bank dan melakukan lebih banyak transaksi online dapat berpeluang menjadi korban *e-mail* phishing. Ketiga adalah pengguna yang tidak menyadari akan bahaya serangan phishing. Faktor yang keempat adalah kebiasaan pengguna dalam menggunakan media. Kebiasaan pengguna mengecek *e-mail* pada saat sarapan pagi, hal ini mengakibatkan kurangnya rasa kecurigaan terhadap email phishing.

Didukung oleh pernyataan Radiansyah et al., (2016) faktor yang membuat pengguna menjadi korban serangan phishing adalah kurangnya pengetahuan korban mengenai informasi kejahatan phishing seperti halnya memdedakan nama domain yang resmi dengan yang palsu, selain itu pengguna tidak memperhatikan indikator keamanan browser. Pengguna tidak mengetahui strategi dalam menghadapi serangan phishing, tidak memberitahukan *e-mail* phishing yang diterima kepada pihak bank serta tidak mengetahui kebijakan bank tentang layanan perbankan online. Selain itu, seringnya pengguna menggunakan kata sandi yang sama pada semua layanan di internet, yang dapat meningkatkan risiko keamanan data bagi pengguna.

Penelitian yang di lakukan oleh Malik & Malik, (2011) mengungkapkan bawa berbagi dan mempublikasikan informasi pribadi pada layanan jaringan sosial itu diperlukan. Namun, hal ini dapat menimbulkan risiko serangan *cyber (*phishing*)* yang memanfaatkan publikasi informasi di layananan jaringan sosial.

Gulo et al., (2021) menyatakan bahwa minimnya pengetahuan pengguna terhadap alat teknologi yang digunakan adalah penyebab terjadinya kejahatan phishing, sehingga pengguna harus dibekali pengetahuan dalam mengoperasikan sebuah teknologi.

Berdasarkan pengetahuan pengguna, Zielinska et al., (2015) mengungkapkan bahwa para ahli (expert) memiliki pemahaman yang lebih luas tentang perkembangan dan karakteristik serangan *e-mail* phishing dari pada pemula. Para alhi dianggap lebih mampu mengambil rsiko dan menghindari ancaman serangan phishing daripada pemula.

Abroshan et al., (2018) mengungkapkan bahwa pelaku menggunakan kelemahan pengguna dengan menawarkan promosi yang menarik serta mengelabui pengguna agar dapat memenuhi keinginan pelaku. Pelaku menargetkan psikologis pengguna, dan menggunakan kelemahan tersebut untuk membangun kepercayaan pengguna. Pelaku menggunakan perilaku psikologis yang ditemukan untuk merancanakan penipuan. Hal ini menyebabkan pengguna dengan mudah terjebak dengan hadiah atau promosi yang di berikan pelaku melalui *e-mail* palsu.

Yang et al., (2022) menyatakan bahwa pengetahuan dan pengalaman merupakan faktor penting dalam mempengaruhi risiko phishing. Terdapat banyak penelitian yang menunjukan bahwa pengetahuan dan pengalaman memiliki dampak yang signifikan terhadap berhasil atau tidaknya serangan phishing. Perilaku keamanan informasi pengguna memiliki hubungan yang relatif tinggi dengan kerentanan phishing. Menganalisis maksud pengguna dalam kaitannya dengan perilaku keamanan. Banyak penelitian telah meneliti karakteristik demografis sebagai faktor penting yang memengaruhi kerentanan terhadap phishing. Gander merupakan faktor yang sangat penting, kerena laki-laki lebih mementingkan hasil instrumental, sedangkan perempuan lebih mementingkan proses. Usia juga memengaruhi kerentanan terhadap phishing.

Alsharnouby et al., (2015) mengungkapkan dalam penelitian nya penulis menkaji kemampuan pengguna dalam menganalisis situs phishing. Responden sebelumnya dilatih tentang ancaman phishing dan fitur keamanan browser yang di tingkatkan. Hasilnya, 53% responden mampu mengidentifikasi ancaman phishing. Hasil ini jauh dari harapan awal bahwa 86% pengguna dapat mengidentifikasi situs phishing. Ini karena pengguna hanya menghabiskan 6% dari waktu mereka untuk memantau indikator keamanan browser dan fokus untuk mengenali tampilan konten situs web yang sedang diiuji.

Penelitian yang dilakukan ohe Button et al., (2014) mencoba mencari tahu mengapa pengguna menjadi korban penipuan online. Ada berbagai penipuan online dengan teknik yang sama yaitu pelaku mencoba mengelabui pengguna dengan menjadi pihak dari lembaga ternama dan website yang menyerupai lembaga terpercaya melalui *e-mail.* Teknik yang digunakan yaitu teknik penipuan marketing dengan membujuk pengguna agar membuka situs palsu. Pengguna akan mendapatkan *e-mail* promosi atau terdapat masalah sehingga pelaku membujuk pengguna untuk melakukan *login* pada *website* palsu yang telah dikirimkan. Pengguna yang mendapatkan *e-mail* akan percaya dan tertarik untuk membuka *website* yang dikirim pelaku melalui *e-mail.*

Hasanah, (2014) menyatakan bawha faktor penyebab terjadinya ancaman serangan phishing dikarenakan minimnya pengetahuan pengguna dalam menjaga keamanan data, minimnya pengetahuan pengguna terhadap ancaman kriminalitas online, kurangnya pengetahan mengenai ancaman phishing.

Arachchilage & Love, (2014) mengungkapkan bahwa pengetahuan proses pengguna dan pengetahuan konseptual dapat mempengaruhi perilaku pengguna dalam menghindari ancaman phishing. Pengetahuan prosedural pengguna dinilai berdasarkan kemampuan pengguna dalam mengidentifikasi situs web phishing dari lima URL yang disediakan, dan pengetahuan konseptual pengguna dinilai dari bagian URL mana yang akan menunjukkan apakah situs web tersebut adalah phishing atau tidak.

Penelitian yang dilakikan oleh (Khairunnisa, 2021) mengungkapkan bahwa penyebab terjadinya phishing pada transaksi *e-commerce* yaitu sistem keamanan platform yang lemah, gambar halaman website/platform sangat mudah untuk ditiru, kurangnya informasi tentang serangan phishing yang di hadapi pengguna, serta kurangnya

pengetahuan pengguna tentang kejahatan phishing, rawannya transaksi *online* terhadap pelanggaran hak konsumen.

Berdasarkan penelitian-penelitian tersebut dapat diketahui bahwa kejahatan phishing masih sering terjadi karena pengetahuan pengguna yang masih minim, menyerang psikologis dengan cara mengelabui korban melalui penawaran promosi dan privasi *social networking services.* Dengan demikian perlu adanya pencegahan serangan phishing pada layanan *e-commerce* guna mengurangi berbagai risiko kerugian konsumen.

3.2 Pencegahan terhadap serangan serangan phishing

Berdasarkan hasil studi literatur yang telah dilakukan sebelumnya, edukasi terhadap ancaman serangan phishing pada saat menggunakan layanan *e-commerce* adalah edukasi terhadap pengguna, psikologis dan privasi *social networking service,* yang dapat digunakan untuk mencegah risio serangan phishing pada saat pengguna menggunakan layanan *e-commerce*.

Mengedukasi pengguna adalah faktor terpenting dalam pencegahan phishing. Pengguna yang memiliki pengetahuan dalam menyadari serangan phishing serta mengetahui langkah-langkah untuk menghindari ancaman tersebut lebih mungki untuk lolos dari ancaman phishing dibandingkan pengguna yang tidak menyadarinya.

Seperti yang diungkapkan oleh Mohammad et al., (2015) edukasi kepada pengguna adalah kunci perlindungan terbaik terhadap ancaman phishing. Pengguna dapat menghindari ancaman ini jika mereka mengetahui indikator keamanan, dapat melihat situs web phishing dan tidak tergiur dengan penawara menarik pada email phishing. Namun, edukasi memerlukan waktu dan biaya yang tinggi di saat phishing terus berkembang. Maka dari itu Mohammad menyarankan dalam mencegah ancaman phishing di perlukan solusi teknis dan solusi hukum.

Hasanah, (2014) mengungkapkan bahwa edukasi kepada pengguna merupakan kunci terbaik dalam menghadapi ancaman phishing. Pengguna yang mengetahui indikator keamanan dapat mendeteksi ancaman phishing sehingga tidak akan tergiur dengan penawaran-penawaran melalui *e-mail,* dengan demikian ancaman tersebut dapat dihindari.

Terdapat banyak teknik, solusi, dan alat yang telah dikembangkan untuk mencegah atau setidaknya mengurangi serangan phishing yang berhasil. Beberapa dari teknik mencoba untuk memblokir *e-mail* atau situs web phishing, sementara yang lain mencoba untuk memberi tahu atau meringatkan pengguna. Ada solusi lain yang tersedia, seperti meningkatkan kesadaran pengguna akan penipuan phishing. Namun, hingga saat ini belum ada solusi yang berhasil sepenuhnya mencegah serangan phishing dan pelaku phishing selalu mengembangkan penipua. Pada saat ini, teknologi anti-phishing tidak dapat mendeteksi atau menghentikan serangan phishing (Abroshan et al., 2018).

Penelitian yang dilakukan Yang et al., (2022) bertuuan untuk menilai efektivias *e-mail* phishing, dan menggunakan model MPSPM untuk memprediksi calon korban phishing. Hasil menunjukkan bahwa model diskriminatif dapat lebih akurat memprediksi calon korban phishing, dan model MPSPM dapat mencapai tingkat deteksi akurat 89,0% pada set penguji. Pengetahuan komputer sangat berkolerasi dengan phishing. Singkatnya, pengetahuan tentang keamanan jaringan adalah salah satu faktor utama yang mempengaruhi kerentanan seseorang terhadap phishing.

Penelitian Volkamer et al., (2017) mengusulkan konsep yang di sebut TORPEDO. Alat ini membantu

pengguna mengidentifikasi tautan phishing yang di sematkan di *e-mail*. Tootlip TORPEDO berisi URL aktuan dengan domain yang disorot. Aktivitas tautan akan tertunda untuk waktu yang singkat, memberikan pengguna waktu untuk memeriksa URL yang sebelumnya telah dikirim. Selain itu, TORPEDO menyediakan bagan informasi yang menjelaskan deteksi phishing. Kami mengevaluasi efektivitas TORPEDO terhadap "status bar" kasus terburuk yang ditawarkan oleh antarmuka webmail lain. Mereka yang menggunakan TORPEDO melakukan secara signifikan lebih baik dalam mendeteksi phishing dan mengidentifikasi *e-mail* yang sah (85,17% *versus* 43,31% jawaban yang benar untuk phishing. Penulis melakukan studi lapangan dengan penggunaan TORPEDO untuk mengeksplorasi pengalaman pengguna TORPEDO di dunia nyata.

Alsharnouby et al., (2015) mengungkapkan 53% pengguna terlatih dapat mengenali situs web phishing. Namun, edukasi yang hanya dilakukan satu kali tidak dapat memebuhi harapan penelitian yang mengharapkan bahwa 86% pengguna dapat mendeteksi situs web phishing.

Arachchilage & Love, (2014) mengembangkan kerangka kerja desain game yang ditujukan untuk meningkatkan kesadaran pengguna tidak hanya akan serangan phishing, tapi juga serangan siber TI lainya seperti virus, malware, botnet, ransomware dan *spyware*.

E-mail adalah media yang rentan untuk serangan phishing. Hal ini serpetu yang di ungkapka oleh Vishwanath et al., (2011) bahwa semakin banyaknya *e-mail* yang di terima pengguna, semakin besar kemungkinan pengguna menjadi calon korban phishing. Risikonya semakin besar juga pengguna tidak hanya menerima *e-mail* dalam jumlah besar, tetapi juga membalas *e-mail* dalam jumlah banyak.

Penelitian yang dilakukan onelh Silic & Back, (2015) mengungkapkan bahwa pengguna perlu diberikan kesadaran akan risiko pengungkapan informasi pribadi di layanan jejaring social. Risiko ini datang dalam bentuk ancaman phishing dan pencurian identitas pengguna.

3.3 Kasus kejahatan phishing di *e-commerce*

Kasus phishing di Indonesia marak terjadi pada *e-commerce* seperti tokopedia, shopee, bukalapak dan sebagainya. Pada tahun 2020 terjadi kasus kejahatan phishing pada layanan *e-commerce* Bukalapak, modus yang di lakukan oleh pelaku yaitu dengan cara menghubungi pengguna melalui aplikasi *whatsapp* dengan mengaku sebagai penjual dan meminta pengguna untuk melakukan konfirmasi barang yang telah dipesan oleh pengguna. Pelaku selanjutnya mengirimkan pesan berupa link untuk mengaktifkan asuransi pengiriman, namun pada kenyataannya link tersebut adalah link phishing. Pengguna menganggap link tersebut adalah link resmi dari pihak bukalapak dan melakukan apa yang pelaku perintahkan, akibat dari hal tersebut pelaku dapat dengan mudah masuk kedalam akun pengguna dan pembelian berubah menjadi terkirim padahal barang yang dipesan belum sampai ke tangan pengguna. Pengguna segera menghubungi pihak bukalapak melaui *live chat* dan *call center*, namun pihak bukalapak tidak bertanggung jawab atas hal tersebut dikarenakan dana yang telah masuk ke dalam akun pelaku sudah tidak ada di bukalapak dan telah digunakan untuk pembayaran pinjaman (Dokubani, 2020).

Kasus kejahatan phishing kembali terjadi di layanan *e-commerce* bukalapak pada tahun 2021, pengguna melakukan pembelian 1 unit sepeda dengan harga Rp 5,25 juta. Pengguna melakukan transaksi berjalan dengan baik, namun di waktu yang sama pelaku mendapatkan sebuah link phishing dari penjual dengan dalih asuransi. Dengan minimnya pengetahuan pengguna terhadap link phishing pengguna langsung percaya dan mengklik link tersebut. Seketika pelaku telah masuk ke dalam akun pengguna dan melakuka pembatalan pesanan, selanjutnya

pelaku melakukan pengiriman uang ke rekening pelaku menggunakan akun pengguna maka secara langsung uang telah terkirim ke rekening pelaku. Pengguna sudah berusaha untuk mengadu kepada pihak bukalapak, namun pihak bukalapak menyatakan tidak bertanggung jawab atas hilangnya dana pengguna sebesar Rp5,25 juta (Ambar, 2020).

Pada tahun 2021 kasus kejahatan phishing terjadi padal layanan *e-commerce* shopee. Modus yang dilakukan pelaku yaitu dengan cara mengirim pesan singkat yang mengaku sebagai penjual dan beralasan bawha jasa pengiriman yang di pilih mengalami gangguan. Sehingga pengguna diminta untuk menggantinya dengan mengklik sebuah link yang telah di kirim pelaku. Pengguna yang tidak menyadari bahwa link tersebut adalah link phishing dengan begitu saja mengklik dan mengisikan data-data apa saja yang pelaku minta. Pada saat itu pelaku langsung masuk kedalam akun shopee pengguna dan total Rp 3 juta di ambil oleh pelaku. Pengguna segera menghubungi *cusoumer service (CS)* shopee dan tidak membutuhkan waktu lama masalah tersebut sudah ditangani oleh pihak *e-commerce* shopee (Faliha, 2021).

Kasus phishing kembali terjadi pada layanan *e-commerce* shopee dengan modus pelaku membatalkan pesanan yang telah dipesan oleh pengguna dengan alasan kepentingan asuransi barang agar barang dapat segera dikirimkan. Pelaku selanjutnya mengirimkan pesan yang berupa link phishing melalui aplikasi *whatsapp* dengan dalih pembayaran melalui link yang pelaku kirim. Sementara pesanan telah dibatalkan oleh pelaku tiga menit sebelum terjadinya transaksi pembayaran. Pengguna sudah melakukan pengaduan kepada pihak shopee terkait kejadian tersebut namun belum ada kejelasan yang pasti dilakukan pihak shopee (Suaib, 2020).

4. KESIMPULAN

Phishing merupakan ancaman yang menggunakan teknik rekayasa sosial dengan menyamar sebagai orang yang berwenang, menjadi penjual ataupun menjadi pihak dari *e-commerce* itu sendiri. Dari sekian banyak *Literature Review*, menyatakan bahwa faktor peyebab terjadinya phishing pada layanan *e-commerce* adalah minimnya pengetahuan pengguna, psikologis serta privasi *social network service.* Dampak dari kejahatan phishing mengakibatkan kerugian finasial, pencurian identitas seseorang dan pembobolan akun. Dengan demikian dilakukanlah pencegahan serangan phishing pada layanan *e-commerce.* Pencegahan yang dilakukan adalah edukasi kepada pengguna, pengguna yang telah mendapatkan edikasi akan dengan mudah mendeteksi dan menghindari ancaman phishing yang terdapat pada *e-mail* dan URL atau situs web. Melakukan pencegahan serangan phishing di level *e-mail*, menggunakan aplikasi (*software)* anti-phishing, serta menggunakan sistem kode verifikasi (OTP) untuk melindungi keamanan informasi dan akun pengguna. Namun, hal ini dikembalikan lagi kepada pengguna apakah akan merespon atau mengabaikan pesan tersebut saat menggunakan transaksi online (*e-commerce*).

DAFTAR PUSTAKA

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2018). Phishing attacks root causes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10694 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-319-76687-4_13

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating

phishing attacks. *International Journal of Human Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Ambar, H. (2020). *Transaksi di Bukalapak terkena Phising, Konsumen Pusing*. Mediakonsumen.Com. https://mediakonsumen.com/2020/07/02/surat-pembaca/transaksi-di-bukalapak-terkena-phising-konsumen-pusing

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*(January 2021), 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Button, M., Nicholls, C. M. N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Creswell, J. W. (2014). *A Concise Introduction to Mixed Methods Research.* SAGE publications.

Dara. (2021). *Akun Shopee Dibajak Penipu Hampir Puluhan Juta Rupiah!* Mediakonsumen.Com. https://mediakonsumen.com/2021/05/01/surat-pembaca/akun-shopee-dibajak-penipu-hampir-puluhan-juta-rupiah

Dokubani, S. (2020). *Terkena Penipuan Lewat Link Phishing di Bukalapak, Bukalapak Sangat Tidak Aman dan Tidak Bertanggung-jawab!* Mediakonsumen.Com. https://mediakonsumen.com/2020/09/22/surat-pembaca/terkena-penipuan-lewat-link-phishing-di-bukalapak-bukalapak-sangat-tidak-aman-dan-tidak-bertanggung-jawab

Faliha, A. (2021). *Cerita Elma Theana Tertipu saat Belanja Online, Alami Kerugian Jutaan Rupiah*. Merdeka.Com.

Ginanjar, A., Widiyansono, N., & Gunawan, R. (2018). Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process. *JUTEI Edisi Volume.2 No.*, *2*(2), 147–157. https://doi.org/10.21460/jutei.2018.22.103

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Hadya Jayani, D. (2021). *Sektor Potensial Ekonomi Digital Indonesia*. Katadata.Co.Id. https://katadata.co.id/ariayudhistira/infografik/61aefade065a4/sektor-potensial-ekonomi-digital-indonesia

Hasanah, F. A. M. (2014). *Ancaman Phising Pada Pengguna Online Banking*. http://ilmusisteminfo.com/upload/file_pdf/ANCAMAN PHISING PADA PENGGUNA ONLINE BANKING 1567491587.pdf

Khairunnisa, A. (2021). *PERLINDUNGAN KONSUMEN DALAM TRANSAKSI E-COMMERCE PLATFORM BUKALAPAK* (Vol. 7). UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH JAKARTA 1441.

Malik, H., & Malik, A. S. (2011). Towards identifying the challenges associated with emerging large scale social networks. *Procedia Computer Science*, *5*, 458–465. https://doi.org/10.1016/j.procs.2011.07.059

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1–24. https://doi.org/10.1016/j.cosrev.2015.04.001

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.

Pratama Afrianto, A., & Irwansyah, I. (2021). Eksplorasi Kondisi Masyarakat Dalam Memilih Belanja Online Melalui Shopee Selama Masa Pandemi Covid-19 Di Indonesia. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *3*(1), 10–29. https://doi.org/10.47233/jteksis.v3i1.181

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1. https://doi.org/10.22219/jibe.vol7.no1.1-14

Silic, M., & Back, A. (2015). The Dark Side of Social Networking Sites: Understanding Phishing Risks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2634887

Suaib, I. (2020). *Modus Penipuan oleh Penjual di Shopee*. Mediakonsumen.Com. https://mediakonsumen.com/2022/01/07/surat-pembaca/modus-penipuan-oleh-penjual-di-shopee-2

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Volkamer, M., Renaud, K., Reinheimer, B., & Kunz, A. (2017). User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers and Security*, *71*(March), 100–113. https://doi.org/10.1016/j.cose.2017.02.004

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting User Susceptibility to Phishing Based on Multidimensional Features. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/7058972

Zielinska, O., Welk, A., Mayhorn, C. B., & Murphy-Hill, E. (2015). Exploring expert and novice mental models of phishing. *ACM International Conference Proceeding Series*, *21-22-Apri*. https://doi.org/10.1145/2746194.2746216