Ekonomika-Bisnis http://ejournal.umm.ac.id/index.php/jeb
Vol. 7 No. 1 Bulan Januari Tahun 2016 Hal 1-14
p-ISSN : 2088-6845 e-ISSN : 2442-8604

ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING

Ikhsan Radiansyah, Candiwan, Yudi Priyadi
Fakultas Ekonomi Bisnis Universitas Telkom
E-mail: *newbieot@student.telkomuniversity.ac.id; candiwan@telkomuniveristy.ac.id; whypi@telkomuniversity.ac.id*

Abstract

The purpose of this study was to determine the factors that cause the emergence of phishing and prevention against phishing threats. Systematic Literature Review methods used to find answers to the research questions by searching for studies related to the threat of phishing in online banking services and perform narrative synthesis on the findings. Minimal knowledge of the user, and the user's psychological privacy of users of social networking services considered as factors that cause phishing. Educating users about the threat of cyber crime, prevention at the level of e-mail, the use of anti-phishing software, and system implementation disposable password in banking services is an effective deterrent to the threat of phishing. Users must have a good knowledge of the threat of crime, especially phishing, and the Bank has the responsibility to provide education related to threats that can harm the user.

Keywords *: Cyber Crime, Information Securit, Online Banking, Phishing*

Abstrak

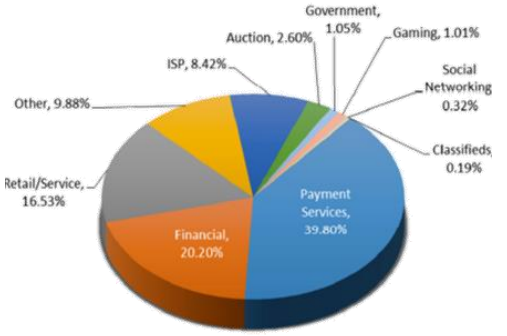
Tujuan penelitian ini adalah mengetahui faktor-faktor penyebab munculnya phishing dan pencegahan terhadap ancaman phishing. Metode Systematic Literature Review dipakai untuk menemukan jawaban atas pertanyaan penelitian tersebut dengan mencari studi-studi yang berhubungan dengan ancaman phishing pada layanan online banking dan melakukan narrative synthesis atas temuan tersebut. Pengetahuan pengguna yang minim, psikologis pengguna dan privasi social networking services pengguna dinilai sebagai faktor-faktor penyebab phishing. Edukasi terhadap pengguna mengenai ancaman kejahatan siber, pencegahan pada tingkat e-mail, penggunaan perangkat lunak anti-phishing, dan implementasi sistem kata sandi sekali pakai pada layanan perbankan merupakan pencegahan efektif pada ancaman phishing. Pengguna (nasabah) harus memiliki pengetahuan yang baik mengenai ancaman kejahatan kriminal khususnya phishing dan Bank mempunyai tanggung jawab untuk memberikan edukasi terkait ancaman yang dapat merugikan pengguna.

Kata kunci : *Cyber Crime, Information Securit, Online Banking, Phishing*

Perkembangan teknologi informasi dan komunikasi (ICT) di dunia sangat dirasakan manfaatnya dalam berbagai sektor Industri, Perbankan maupun Usaha Kecil Menengah (UKM). Sektor-sektor tersebut mera-sakan manfaat efisiensi dan efektivitas dalam segi operasional maupun peningkatan layanan terhadap pengguna. Namun perkembangan tersebut memunculkan tantangan baru dengan munculnya berbagai tindak kriminal berbasis siber (*cyber crime*) oleh pihak-pihak yang berusaha mengeksploitasi kelemahan sistem dan kesadaran pengguna terhadap Sistem Informasi.

Salah satu bentuk *cyber crime* yang dilakukan oleh para *frauder* adalah *Phishing*. *Phishing* adalah kegiatan kriminal dengan menggu-nakan teknik rekayasa sosial. *Phisher* (sebutan bagi pelaku kriminal *phishing*) berupaya menipu untuk mendapatkan informasi sensitif, seperti *username*, *password* dan rincian kartu kredit, dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik (N. P. Singh, 2007). *Phishing* menyerang semua sektor industri berbasis *online*, seperti *e-commerce*, sosial media dan perbankan. Tindakan *phishing* mengincar informasi sensitif pengguna untuk digunakan oleh pihak yang tidak berwenang. Pengguna dirugikan dalam hal privasi, penya-lahgunaan (eksploitasi) dari tindakan *hacking* bahkan kerugian finansial.

Layanan pembayaran (*payment service*) menjadi sektor industri yang paling ditargetkan pada kuartal kedua 2014, dengan 39,80 persen dari serangan selama periode tiga bulan dari April sampai Juni 2014, seda-ngkan jasa keuangan (*financial*) terus mengikuti dengan 20,20% (Anti-Phishing Working Group, 2014). Ini terlihat dalam pie-chart pada Gambar 1.



Gambar 1. Keseluruhan Statistik untuk serangan phishing, April-Juni 2014

Sektor Finansial merupakan sa-lah satu target eksploitasi oleh para *frauder*. Perbankan sebagai layanan transaksi keuangan massal tidak luput dari *cyber crime* yang dilakukan *frauder*. *Phishing* dapat menggunakan halaman website palsu untuk menge-labui dan mencuri data-data pribadi pengguna.

Phishing tidak hanya menyerang Indonesia saja. Pada tahun 2013, Sera-ngan *Phishing* menyebabkan kerugian finansial sebesar $ 5,9 Milyar (Rp 80,328 Triliun) di dunia berdasarkan laporan EMC (EMC, 2014). Serangan *Phishing* tidak hanya menimbulkan kerugian finansial saja. Phishing me-nyebabkan konsekuensi serius terhadap kehilangan data pribadi pengguna, dan kerugian nama merk perusahaan yang tercemar akibat kasus *phishing* (Symantec Brightmail TM, 2014).

Berbagai kasus *phishing* terhadap dunia *financial service* (perbankan) di dunia mendorong akademisi untuk melakukan penelitian terhadap sera-ngan *phishing*. Telah banyak studi penelitian dengan topik *phishing* yang berhubungan dengan deskripsi sera-ngan, tipe-tipe *phishing* dan pence-gahan terhadap *phishing*. Studi tersebut

dibuat dalam waktu yang berbeda-beda, pada lingkungan (tempat) yang berbeda dan fenomena yang berbeda juga.

Oleh karena itu, peneliti tertarik menganalisis ancaman *phishing* dalam layanan *online banking* berdasarkan metode *systematic literature review* dengan fokus terhadap dua tujuan penelitian yaitu menganalisis faktor yang memungkinkan ancaman phising muncul ketika pengguna menggunakan online banking dan memberikan rekomendasi pencegahan terhadap ancaman *phising*.

Metode Penelitian

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR). *Systematic Literature Review* (SLR) atau juga disebut *Systematic Review* adalah *literature review* yang umumnya dilakukan oleh peneliti untuk memecahkan masalah dari penelitian. Awalnya teknik penelitian ini digunakan untuk mencari keefektifitas dari layanan kesehatan namun sekarang teknik ini dapat juga digunakan dengan topik lebih luas.

Tujuan SLR adalah untuk mensintesis temuan penelitian dari sejumlah besar studi yang berbeda pada intervensi tertentu atau isu yang kemudian dapat berpotensi digunakan untuk menginformasikan kebijakan dan praktek di bidang diselidiki (Ridley, 2012). Penelitian ini mengambil studi sebanyak 83 literatur dan setelah dilakukan *filtering* (analisis data) jumlah studi berkurang menjadi 37 literatur. Langkah-langkah yang dilakukan adalah sebagai berikut:

Pertama, Wawancara terhadap narasumber (*expert*). Berkonsultasi pada pakar yang mempunyai pengalaman di bidang *Information Security*. Penelitian ini melibatkan akademisi dan Praktisi dalam bidang *Information Security*. Richi Aktorian yang berprofesi sebagai Senior Manager of IT Resilience & Security pada PT Bank Mandiri (Persero) Tbk, Surya Michrandi Nasution yang berprofesi sebagai dosen Fakultas Teknik Elektro pada Telkom University. Beliau mengajarkan bidang Information Security pada Security lab. Memiliki pengetahuan terkait pada bidang keamanan informasi dan pernah memiliki CEH (*certified ethical hacking*) dan Yudha Purwanto yang berprofesi sebagai dosen Fakultas Teknik Elektro pada Telkom University dan Konsultan IT pada beberapa perusahaan. Beliau mengajarkan bidang Information Security pada Security lab. Memiliki pengetahuan terkait pada bidang keamanan informasi dan memiliki CEH (*certified ethical hacking*).

Kedua, Melakukan Pencarian Studi. Pencarian bukti/fakta pada sumber yang terpercaya yaitu Elsevier, IEEE, ACM, dan Sage. Bukti/fakta berupa research paper. Setiap research paper yang telah diunduh dan dibaca dilakukan dokumentasi mengenai judul literatur, nama penulis, tahun paper dan ringkasan penelitian. Pencarian dilakukan pada research paper yang dipublikasikan dengan dengan meng-gunakan kata kunci "*phishing, online banking, man-in-the-middle, man-in-browser, cyber crime, online banking phishing*". Kata kunci tersebut ditentukan melalui wawancara kepada praktisi (Richi Aktorian). Pada tahap ini telah ditemukan 83 research paper atas pencarian tersebut.

Ketiga, Ekstraksi Data Studi. Pada tahap ini yaitu memilah dan mengambil data yang berhubungan dengan topik penelitian dari research paper yang telah dibaca. Data Ekstraksi

disajikan dalam bentuk tabel ringkasan informasi yang telah diekstrak dari studi yang telah dipilih.

Keempat, Menilai kelayakan studi. Jurnal/Studi yang dijadikan landasan penelitian ditelusuri kelayakannya. Setiap research paper yang dijadikan landasan, harus memiliki jawaban "ya" terhadap tiga pertanyaan di bawah ini: 1) Apakah studi memiliki fokus pertanyaan yang jelas?; 2) Apakah studi menggunakan metode yang valid untuk menjawab pertanyaan penelitiannya?; 3) Apakah hasil valid yang berasal dari studi penting untuk dijadikan landasan? Setelah dilakukan kelayakan studi, didapatkan 37 research paper yang layak untuk dijadikan landasan untuk menjawab pertanyaan penelitian.

Kelima, Data Sintesis yaitu menggunakan teknik narrative *synthesis* sebagai pendekatan tekstual yang menyediakan analisis hubungan dalam dan di antara studi dan penilaian secara keseluruhan dari bukti. Sebuah sintesis narasi (*narrative synthesis*) dapat dilakukan di mana studi terlalu beragam secara metodologi.

Setiap fakta yang didapatkan dari research paper dan hasil wawancara dibandingkan dan dicocokan satu dengan yang lain. Jika antara paper A dan paper B memiliki kesamaan fakta/bukti temuan penelitian maka fakta/bukti tersebut layak untuk dijadikan landasan penelitian ini. Fakta/bukti temuan yang diperlukan dalam penelitian ini adalah faktor penyebab phishing dan rekomendasi pencegahan phishing pada layanan online banking.

Keenam, Membuat laporan hasil studi. Hasil laporan disajikan dalam bentuk narrative synthesis dilengkapi kesimpulan penelitian yang telah dilakukan, dalam hal ini penelitian harus dapat menjawab faktor-faktor yang memungkinkan Ancaman Phising muncul ketika pengguna menggunakan online banking dan memberikan rekomendasi

Hasil Penelitian dan Pembahasan

Phishing pada layanan online banking merupakan ancaman menggunakan teknik rekayasa sosial dengan mengelabui pengguna (nasabah). Pengguna tertarik terhadap penawaran-penawaran melalui e-mail, pesan sing--kat, telepon dari pelaku kriminal yang menyamar sebagai entitas bank resmi dan mengajak nasabah untuk memberikan data-data sensitif terkait data pengguna bank tersebut (Nasution, 2016).

Pada penelitian ini akan dijelaskan mengenai faktor penyebab munculnya ancaman *phishing* ketika pengguna menggunakan layanan online banking dan pencegahan terhadap ancaman tersebut.

Berdasarkan hasil studi literatur yang telah dilakukan sebelumnya, faktor penyebab munculnya ancaman serangan phishing ketika pengguna menggunakan layanan online banking adalah minimnya pengetahuan pengguna, psikologis dan privasi social networking services pengguna. Tabel 1 menunjukkan faktor-faktor penyebab phishing dari berbagai studi yang telah dibaca.

Dhamija, Tygar, & Hearst (2006) mengungkapkan bahwa pengguna dianggap tidak memiliki pengetahuan yang baik mengenai sistem komputer terutama membedakan domain yang resmi dan palsu. Pengguna juga tidak dapat mengenali indikator-indikator keamanan seperti mengecek sertifikat SSL pada browser ketika mengunjungi suatu situs pada internet.

Tabel 1. Faktor penyebab phishing berdasarkan *study literature*

No.	Nama Penulis dan Tahun	Faktor penyebab phishing
1	(Dhamija, et al., 2006)	Pengetahuan pengguna minim dan psikologis
2	(Alsharnouby, et al., 2015)	Pengetahuan pengguna minim
3	(Arachchilage & Love, 2014)	Pengetahuan pengguna minim
4	(Mohammad, et al., 2015)	Pengetahuan pengguna minim
5	(Parmar, 2012)	Pengetahuan pengguna minim, psikologis dan privasi *social networking services*.
6	(Meulen, 2013)	Psikologis
7	(Sein, 2011)	Pengetahuan pengguna minim
8	(Vishwanath, et al., 2011)	Psikologis
10	(Button, et al., 2014)	Psikologis
11	(Zielinska, et al., 2015)	Pengetahuan pengguna minim
12	(USE Act, 2010)	Pengetahuan pengguna minim
13	(Hilley, 2006)	Pengetahuan pengguna minim
14	(Elsevier Advanced Technology, 2015)	Psikologis dan pengetahuan pengguna minim
15	(Malik & Malik, 2011)	Privasi *social networking services*

Pengguna yang mengetahui hal-hal tersebut juga rawan ketika sebuah website phishing menyerupai website resmi (*visual deception*) yang mengakibatkan tidak memperhatikan indikator keamanan pada browser (SSL certified icon).

Faktor pengetahuan dan kesa-daran pengguna terhadap ancaman serangan phishing juga didukung oleh Alsharnouby, Alaca, & Chiasson (2015). Dalam paper tersebut penulis meneliti mengenai kemampuan pengguna untuk mengiden-tifikasi website phishing. Subjek penelitian (responden) sebelumnya telah dibekali oleh edukasi mengenai ancaman phishing dan *improved browser security indicators*. Hasilnya adalah 53% responden berhasil mengidentifikasi ancaman *phishing*. Hasil tersebut dibawah ekspektasi awal yaitu diharapkan 86% pengguna berhasil mengidentifikasi *website phishing*. Hal ini dikarenakan pengguna hanya meng-gunakan 6% waktunya untuk meng-amati indikator keamanan pada browser dan fokus mengenali tampilan konten pada website yang diuji.

Arachchilage & Love (2014) mengungkapkan hal serupa bahwa pengetahuan prosedural dan pengetahuan konseptual pengguna mempengaruhi tin-dakan pengguna untuk menghindari an-caman *phishing*. Pengetahuan prosedural pengguna dinilai dari kemampuan peng-guna untuk mengidentifikasi website *phishing* dari 5 URL yang telah diberikan dan pengetahuan konseptual pengguna dinilai dari bagian URL mana yang menan-dakan website tersebut phishing atau tidak.

Hal ini didukung oleh pernyataan Mohammad, Thabtah, & McCluskey (2015) faktor mengapa pengguna menjadi korban serangan *phishing* adalah mayoritas pengguna memiliki pengetahuan yang minim terhadap ancaman kriminalitas online, tidak memiliki pengetahuan yang baik mengenai ancaman *phishing*, tidak memiliki strategi yang baik dalam mengenali serangan *phishing*, fokus ter-hadap konten dibandingkan indikator pada website, dan tidak mengetahui prosedur layanan online yang dipakai sehingga terjebak ketika mendapatkan e-mail dari layanan online yang mereka gunakan terkait informasi *maintenance* dan infor-masi-informasi lainnya yang dimanfaatkan phisher untuk mendapatkan data-data sensitif pengguna.

Parmar (2012) menyatakan serangan *spear-phishing* yang berbeda dengan serangan phishing konvensional

juga sukses dilakukan akibat pengetahuan psikologis pengguna yang mudah mempercayai situs jejaring sosial. *Spear-phishing* berbeda dari serangan konvensional dimana phisher tidak melakukan bulk e-mail kepada sasarannya namun mengirimkan e-mail *phishing* kepada sasaran potensial yang memiliki tingkat kesuksesan dan timbal balik yang lebih tinggi. Jika pada *phishing* biasa *phisher* menyamar sebagai entitas resmi maka pada *spear-phishing*, *phiser* menyamar sebagai individu/entitas yang diketahui dan digunakan oleh calon korban. Teknik ini umumnya digunakan agar korban mengunduh malware yang terlampir pada e-mail tidak seperti teknik *phishing* konvensional yang mengarahkan korban pada website palsu. *Phisher* mendapatkan data-data sensitif pengguna melalui sosial media lalu memanfaatkannya untuk mengelabui pengguna. Terbukti teknik *spear-phishing* memiliki tingkat kesuksesan 19% dibandingkan teknik *phishing* konvensional yang hanya memiliki tingkat kesuksesan 5%.

Malik & Malik, (2011) dalam penelitiannya mengungkapkan bahwa berbagi informasi pribadi dan mengungkapkannya pada SNS (*social networking services*) adalah sebuah kebutuhan. Namun hal tersebut beresiko terhadap serangan siber (termasuk *phishing*) yang memanfaatkan keterbukaan informasi pribadi pada SNS.

Meulen (2013) menyatakan tanggung jawab atas terjadinya kasus penipuan online pada layanan online banking tidak hanya dipegang oleh pihak bank saja namun pengguna turut bertanggung jawab atas terjadinya kasus tersebut. Pengguna dinilai lalai dan mengabaikan peraturan yang telah diedukasikan oleh pihak bank. Sebagai contoh terdapat kasus dimana korban mendapatkan e-mail *phishing* dan telepon mengatasnamakan Rabobank, bank dimana pengguna menggunakan layanan online banking. Pengguna mendapatkan telepon yang berasal dari representatif Rabobank (phisher) dan menanyakan e-mail yang diterima oleh pengguna. *Phisher* mengatakan akun pengguna perlu di cek dan diklarifikasi untuk menghindari masalah potensial akibat dari e-mail yang telah diterima. Pengguna diminta memberikan informasi kredensial seperti kode random atau identitas untuk melakukan transaksi. Atas informasi inilah phiser dapat melakukan transaksi dengan menggunakan akun pengguna. Pengguna yang lalai dengan tidak mengklarifikasi telepon tersebut kepada pihak bank dan tidak mengetahui peraturan permintaan informasi sensitif pada bank menyebabkan kasus tersebut terjadi.

Hal lainnya yang membuat pengguna terjebak dalam serangan phishing adalah sifat naif pengguna dalam menggunakan layanan perbankan para internet. Pengguna umumnya menggunakan password yang sama untuk berbagai halaman website dan password yang digunakan tidak jauh nama anak, nama peliharaan, tempat lahir, dan tanggal ulang tahun ungkap Sein (2011).

Hal serupa dikemukakan juga oleh Vishwanath, Herath, Chen, Wang, & Rao (2011) bahwa pengguna merupakan faktor utama terjadinya penyebab *phishing*. Terdapat 4 alasan mengapa pengguna menjadi korban *phishing*. Pertama adalah semakin banyak e-mail yang diterima pengguna maka semakin besar peluang mereka ditipu. Kedua adalah pengguna umumnya akan membuka e-mail dari entitas yang mereka ketahui. Pengguna yang memiliki hubungan lebih dari satu lembaga bank dan melakukan transaksi online yang lebih banyak dibandingkan lainnya mereka berpeluang menjadi korban e-mail *phishing*. Yang ketiga adalah pengguna yang tidak mengetahui ancaman serangan *phishing*. Faktor keempat adalah

kebiasaan dalam penggunaan media. Seseorang yang mempunyai kebiasaan mengecek e-mailnya setiap pagi sambil sarapan. Kebiasaan ini mengurangi rasa curiga dan berpeluang membuka dan mempercayai *surel phishing*.

Penelitian yang dilakukan oleh Button, Nicholls, Kerr, & Owen (2014) mencoba mencari tau mengenai mengapa korban jatuh kepada penipuan online. Terdapat beragam penipuan online namun dengan teknik yang sama yaitu kriminal mencoba menjadi entitas yang sah berupa e-mail dari lembaga ternama dan website yang menyerupai lembaga terpercaya. Teknik yang digunakan untuk mengajak pengguna membuka situs web palsu tersebut seragam yaitu menggunakan teknik penipuan marketing. Pengguna mendapatkan e-mail mengenai promosi transaksi dengan waktu terbatas atau menginformasikan bahwa akun pengguna mempunyai masalah dan dibutuhkan login kembali pada website resmi namun palsu. Pengguna yang mendapatkan e-mail tersebut tertarik dan membuka website phishing yang telah disediakan pada e-mail.

Dilihat dari pengetahuan pengguna, Zielinska, Welk, Mayhorn, & Murphy-Hill (2015) mengung-kapkan bahwa para ahli (expert) cenderung memiliki pemahaman yang lebih komprehensif tentang bagaimana tren serangan phishing dan karak-teristiknya melalui e-mail dibandingkan pemula. Para ahli dinilai lebih dapat mengambil resiko dan meng-hindari ancaman serangan phishing dibandingkan pengguna pemula.

Selain menggunakan website palsu,kejahatan kriminal dengan menggunakan teknik phishing juga memanfaat malware untuk mencuri data pribadi pengguna. Seperti yang diungkapkan USE Act (2010) Serangan baru Zeus Malware yang berbasis botnet juga menyerang pengguna kartu kredit di Amerika Serikat. Serangan Zeus menggunakan teknik *man-in-the-middle* dengan pop-up meminta untuk memberikan informasi sensitive pada website yang resmi. (Hilley, 2006) menyatakan bahwa pengguna tidak sadar mengunduh malware ketika mengunjungi situs berbau pornografi, situs yang menyediakan konten ba-jakan dan ketika membuka e-mail phishing.

Malware yang berada di komputer pengguna memiliki resiko ancaman yang lebih tinggi dibandingkan phishing konvensional. IBM menyatakan penipuan pada mayoritas bank disebabkan oleh teknik rekayasa sosial untuk menggagalkan sistem dua faktor autentikasi. Teknik ini menggunakan trojan "*The Dyre*" dimana malware tersebut menginjeksi halaman web palsu pada situr resmi. Halaman web palsu tersebut menginformasikan bahwa situs sedang mengalami perbaikan dan pengguna diharapkan menghubungi nomor telepon yang tertera pada halaman. Ketika pengguna menelpon nomor tersebut, pengguna akan dimintai data-data sensitif terkait bank tersebut diungkapkan oleh Elsevier Advanced Technology (2015).

Berdasarkan hasil studi literatur yang telah dilakukan sebe-lumnya, pencegahan terhadap ancaman serangan phishing ketika pengguna menggunakan layanan online banking adalah edukasi terhadap pengguna, psikologis dan privasi *social net-working services* pengguna dan penggunaan sistem one time password pada perbankan.

Edukasi kepada pengguna merupakan faktor terpenting dalam pencegahan *phishing*. Pengguna yang memiliki pengetahuan dan kesadaran mengenai serangan phishing dan mengetahui tindakan untuk meng-hindari ancaman tersebut rentan lolos menghindari ancaman *phishing* dibandingkan pengguna yag tidak mengetahuinya.

Seperti yang diungkapkan oleh Alsharnouby, Alaca, & Chiasson (2015) 53% pengguna yang telah dibekali edukasi

mampu mendeteksi website phishing. Namun edukasi yang hanya dilakukan satu kali belum mampu memenuhi ekspektasi pene-litian yang mengharapkan 86% peng-guna mampu mendeteksi website *phishing.*

Mohammad, Thabtah, & McCluskey (2015) juga mengatakan bahwa edukasi kepada pengguna merupakan kunci pencegahan terbaik untuk menghadapi ancaman phishing. Jika pengguna mengetahui indikator keamanan, dapat mendeteksi websie *phishing* dan tidak tergiur pada penawaran menarik pada e-mail *phishing* maka ancaman tersebut dapat dihindari. Namun edukasi membutuhkan waktu dan biaya yang tinggi sementara phishing terus berkembang. Sehingga Mohammad menyarankan perlunya solusi teknis dan solusi hukum untuk mencegah ancaman phishing.

Teknik *spear-phishing* yang lebih beresiko dibandingkan teknik phishing konvensional juga menyarankan edukasi pengguna sebagai pencegahan terbaik. Diungkapkan oleh Parmar (2012) CSCIC (*Cyber Security and Critical Infrastructure Coordination*) mengedukasi serangan phishing kepada para pegawai negeri di Amerika Serikat menggunakan e-mail. Pada awalnya 15% pengguna meng-inputkan passwordnya pada halaman website palsu sebelum diberi perin-gatan bahwa e-mail tersebut adala pelatihan phishing dan menjelaskan kesalahan atas tindakan mereka (pengguna). Empat bulan kemudian CSCIC kembali mengirimkan e-mail phishing kepada pegawai negeri di Amerika Serikat dan hasilnya hanya 8% pengguna yang mencoba berinteraksi ke halaman website palsu.

Pengetahuan mengenai phishing dan pencegahannya dapat diperoleh melalui edukasi, kesadaran dan pengalaman. Diperlukannya kolaborasi atas tiga aspek tersebut untuk meningkatkan *self efficacy* pada pengguna seperti yang diungkapkan oleh Vishwanath et al. (2011).

Pihak bank mempunyai kewajiban untuk memberikan informasi mengenai *phishing* dan pencegahannya kepada pengguna. Studi yang dilakukan pada Bank di hongkong, Bank menyediakan fasilitas online banking memuat informasi mengenai phishing dan tindakan anti-*phishing* pada pada halaman resmi websitenya. Akses kepada informasi mengenai phishing lebih mudah dilakukan dibandingkan tindakan anti-*phishing*. Pada Bank di Hongkong, tindakan pencegahan terhadap ancaman phishing melalui surat elektronik lebih sulit diakses dibandingkan ancaman *phishing* dalam bentuk *malware* (Bose & Leung, 2008).

Efektifitas pelatihan pencegahan *phishing* (*embedded training*) dapat membandingkan dengan pesan keamanan pada umumnya. Hasilnya adalah pelatihan dinilai lebih baik dibandingkan mengi-rimkan pesan keamanan kepada pengguna. Mereka berkesimpulan bahwa pelatihan pencegahan *phishing* (*embedded training*) membantu pengguna mempelajari menge-nai bahaya *phishing* dan cara untuk menghindarinya (Kumaraguru, et al., 2007).

Pada *research paper* yang berbeda telah mengungkapkan bahwa efektivitas pengguna dalam mempelajari materi *phishing* lebih baik ketika pengguna telah mengalami simulasi serangan (*embedded*) dibandingkan ketika pelatihan dikirimkan melalui e-mail (*non-embedded*). Pengetahuan pengguna lebih bertahan setelah *embedded training* dibandingkan non-*embedded training* (Kumaraguru, et al., 2007).

Selain itu, penelitian yang berfokus mengedukasi pengguna dan membantu mereka untuk menghindari serangan phishing. Mereka mengembangkan pelatihan *embedded system* dengan nama PhishGuru dengan masa pelatihan 28 hari. Pelatihan ini terbukti efektif ketika pengguna yang telah dilatih dibandingkan

dengan pengguna yang belum dilatih oleh PhishGuru (Kumaraguru, et al., 2009). Lalu dilan-jutkan dengan membuat permainan bernama Anti-Phishing Phil yang bertujuan memberikan edukasi kepada pengguna agar dapat mendeteksi URL resmi dan palsu. Hasilnya adalah walaupun anti-phishing software ber-tindak sebagai garis pertama dalam menghadapi serangan phishing namun edukasi pengguna menawarkan pendekatan yang membantu pengguna mengidentifikasi e-mail dan website palsu (Kumaraguru, et al., 2010).

Edukasi pengguna melalui media permainan (game) dinilai efektif dan meningkatkan self efficacy peng-guna dalam menghindari penipuan online. Arachchilage & Love (2014) merancang kerangka desain permainan yang diha-rapkan tidak hanya dapat meningkatkan kesadaran pengguna terhadap serangan phishing namun serangan siber IT lainnya seperti virus, *malware, botnet* dan *spyware*.

Adapun mengenai faktor privasi pada *social networking sites*, penelitian lain mengungkapkan bahwa pengguna harus diberikan edukasi mengenai resiko ketika mengungkapkan informasi pribadi di *social networking services*. Resiko tersebut berupa ancaman phishing dan pencurian identitas pribadi pengguna (Silic & Back, 2016).

Sebelumnya telah dijelaskan mengenai faktor-faktor penyebab *phishing* diantaranya akibat pengetahuan pengguna yang minim, kebiasaan pengguna, psikologis pengguna dan keterbukaan privasi *social networking services* pengguna. Empat faktor tersebut dapat diatasi melalui edukasi kepada pengguna dikarenakan empat faktor tersebut berasal dari pengguna sendiri.

Pengetahuan pengguna yang minim atas ancaman kejahatan siber (khususnya *phishing*), psikologis dan keterbukaan *social networking services* diatasi melalui edukasi yang dilakukan oleh bank. Media edukasi dapat disampaikan melalui berbagai cara namun bank harus fokus pada efektivitas edukasi tersebut. Seperti yang diungkapkan oleh Kumaraguru, et al. (2009) bahwa edukasi yang efektif dilakukan dengan sistem pelatihan (*embedded training*). Namun sistem tersebut membutuhkan waktu dan biaya yang besar untuk dilakukan. Adanya media edukasi lain dalam bentuk permainan, edukasi melalui halaman website, video edukasi dan lain sebagainya. Bentuk edukasi yang akan diberikan kembali kepada pihak bank dengan memperhitungkan biaya serta timbal balik atas tindakan tersebut.

Namun pihak bank tidak hanya menjadi pemegang tanggung jawab atas ancaman kejahatan ini. Pengguna turut berperan dan bertanggung jawab atas tindakan yang mereka lakukan dalam menghadapi ancaman phishing. Sehingga pengguna juga harus membekali dirinya mengenai pengetahuan dalam kejahatan siber (khususnya *phishing*) dan waspada dalam menggunakan layanan online banking.

Selain website, e-mail merupakan media yang rawan terhadap serangan phishing. Hal ini seperti diungkapkan oleh Vishwanath, Herath, Chen, Wang, & Rao (2011) bahwa semakin banyak e-mail yang diterima oleh pengguna maka semakin rawan pengguna menjadi calon korban phishing. Resiko akan semakin besar jika pengguna tidak hanya menerima e-mail dalam volume besar namun juga merespon e-mail dalam volume yang besar juga.

Phishing dapat dicegah melalui pemasangan filter yang mengklasi-fikasikan e-mail menjadi dua kategori yaitu asli (*legitimate*) dan palsu (*fraudulent*) (Castillo, et al., 2007). Penggunaan fungsi filter, perusahaan dapat melindungi pegawai dan pelanggannya dari e-mail spam yang mengancam mencuri data pengguna e-mail.

Jika phiser mengetahui target calon korban dan menggunakan teknik spear phishing maka filter e-mail spam dan phishing menjadi tidak efektif. Parmar (2012) mengatakan hal ini dikarenakan spear-phishing melakukan pendekatan yang berbeda dibandingkan *phishing* konvensional yang mudah terdeteksi oleh filter.

Solusi lainnya untuk mencegah *phishing* pada tingkat e-mail adalah pengguna internet seharusnya menggunakan fasilitas Tanda tangan digital pada e-mail atau *Digital Signature E-mail* (Garfinkel, et al., 2005). Tanda tangan digital menggunakan kunci *asimetric kriptografi* seperti RSA yang memungkinkan pengguna untuk membedakan identitas sang pengirim e-mail. Namun hal ini akan menjadi masalah ketika pengguna yang menggunakan satu komputer untuk mengakses akun e-mailnya.

Pencegahan terhadap ancaman serangan *phishing* juga dapat menggunakan perangkat lunak *anti-phishing* selain indikator keamanan pada browser seperti penggunaan protokol HTTPS (*SSL certifed*) pada situs.

Ekstensi browser yang bernama AntiPhish. AntiPhish bertujuan untuk melindungi pengguna dari halaman website palsu dengan menampilkan pesan waspada ketika pengguna mencoba menginput data sensitif (username, password) pada halaman yang tidak terpercaya. Namun AntiPhish saat ini hanya berupa *prototype* (Kirda & Kruegel, 2005).

Selain itu, dapat juga menggunakan GoldPhish, sebuah plugin yang terpasang pada browser bertujuan untuk melindungi pengguna dari *zero-day phishing sites*. Pence-gahan terhadap phishing umumnya dilakukan dengan memakai teknik blacklist maupun whitelist terhadap URL phishing yang telah dideteksi namun teknik ini tidak efektif ketika berhadapan dengan zero-day attack. Phisher selalu lebih terdepan membuat website palsu yang tidak dapat dideteksi oleh anti-phishing berbasis blacklist/whitelist, GoldPhish menawarkan solusi dengan pendekatan teknik Heuristic dengan menangkap gambar dari halaman website lalu menggunakan *optical character recognition* untuk mengubah gambar ke teks lalu diintegrasikan dengan *algoritma Google Pagerank* yang membantu untuk menentukan apakah website tersebut valid atau tidak. GoldPhish diklaim akurat dalam mendeteksi 100% website asli dan 98% mendeteksi website phishing (Dunlop, et al., 2010).

Sistem perbankan juga harus menggunakan sistem *One Time Pass-word* (OTP). Saat melakukan transaksi pada layanan online, institusi perba-nkan memberikan perangkat token kepada pelanggan yang dapat mengeluarkan PIN atau *One Time Password* (OTP) yang dikirimkan melalui pesan teks kepada pelanggan (Nilsson, et al., 2006).

Password sekali pakai (*one time password*) adalah sistem autitentikasi dimana pengguna ketika melakukan login menggunakan password sekali pakai yang dikirimkan melalui aplikasi instant messaging atau sms. Tidak menggunakan password statis, namun sistem password ini hanya sekali pakai (OTP) diungkapkan dalam penelitian (Huang, et al., 2011).

Peretas menemukan celah keamanan dalam penggunaan pera-ngkat token pada layanan online banking. Seperti Malware bernama Gameover Zeus yang telah berada di komputer pengguna melakukan serangan *Man-in-the-Browser* (MitB) dengan teknik *Load Inject Script* yang mampu menambahkan *scipt* (pop-up) pada halaman website resmi dan mencuri informasi kredensial peng-guna seperti PIN Token yang diinputkan pengguna (Tanujaya, 2015).

IT Security Manager salah satu Bank di Indonesia membenarkan ancaman tersebut. Beliau mengatakan Bank mela-

kukan tindak pencegahan melalui tiga aspek yaitu *people, process, technology*. Beliau menga-takan layanan online banking di Indonesia telah memperingatkan pengguna dengan memasang pesan waspada. Bank Mandiri memasang pesan waspada yang berbunyi "Hentikan transaksi jika anda diminta sinkronisasi token pada saat login dan pastikan komputer anda bersih dari virus". Bank BCA memasang pesan waspada "Waspada virus trojan, malware dan spyware. Stop! Jika anda menemukan hal yang tidak biasa pada saat bertransaksi Internet Banking, Stop jangan dilanjutkan!" (Aktorian, 2015).

Namun pesan waspada tersebut kembali ke pengguna apakah memperhatikan dan sadar terhadap pesan tersebut. Meulen (2013) mengungkapkan kejahatan kriminal dalam layanan online terjadi salah satunya akibat pengguna dinilai lalai dan mengabaikan peraturan yang telah diedukasikan oleh pihak bank.

Penutup

Phishing merupakan ancaman yang menggunakan teknik rekayasa sosial (*social engineering*) yang mengelabui pengguna dengan cara menyamar sebagai entitas yang resmi. *Phishing* menyerang berbagai sektor industri termasuk industri perbankan yang menjadi sasaran terbesar. Faktor penyebab phishing pada layanan online banking yaitu Pengetahuan pengguna yang minim, Psikologis, dan Privasi *sosial networking services*.

Oleh karena itu, pencegahan serangan phishing pada Layanan Online Banking dapat dilakukan melalui Edukasi pengguna, pencegahan *Phishing* pada tingkat e-mail, penggunaan perangkat lunak anti-phishing, penggunaan sistem OTP pada sistem perbankan.

Namun untuk OTP melalui perangkat token, peretas menggunakan serangan malware trojan (*Gameover Zeus*) untuk mendapatkan kombinasi PIN pengguna. Trojan tersebut melakukan serangan *Man-in-the-Browser* (MitB) dengan teknik *LoadInjectScript* yang mampu menambahkan scipt (pop-up) pada halaman website resmi dan mencuri informasi kredensial pengguna seperti PIN Token yang diinputkan pengguna.

Perbankan di Indonesia mence-gah hal tersebut dengan memasang pesan waspada yang berbunyi "Waspada virus trojan, malware dan spyware. Stop! Jika anda menemukan hal yang tidak biasa pada saat bertransaksi *Internet Banking*, Stop jangan dilanjutkan!". Akan tetapi, semuanya kembali ke pengguna, memperhatikan atau mengabaikan pesan tersebut ketika menggunakan layanan *online banking*.

DAFTAR PUSTAKA

Aktorian, R., 2015. *Ancaman Siber dalam Online Banking* [Wawancara] (12 January 2015).

Alsharnouby, M., Alaca, F. & Chiasson, S., 2015. Why phishing still works: user strategies. *Int. J. Human-Computer Studies.*

Anti-Phishing Working Group, 2014. *Phishing Activity Trends Report, 2nd Quarter*, Washington D.C: Anti-Phishing Working Group (APWG).

Arachchilage, N. A. G. & Love, S., 2014. Security awareness of computer users: A phishing threat avoidance. *Computers in Human Behavior 38 (2014) 304–312.*

Bose, I. & Leung, A. C. M., 2008. Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decision Support Systems 45*, p. 897–912.

Button, M., Nicholls, C. M., Kerr, J. & Owen, R., 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology 2014 Vol. 47(3),* p. 391–408.

Castillo, M., Iglesias, A. & Serrano, J., 2007. Detecting phishing e-mails by heterogeneous. *H. Yin et al. (Eds.): IDEAL 2007, LNCS 4881,* pp. 296-305.

Courtesy of Computer Associates, 2014. *Types of Phishing Attacks.* [Online] Available at: http://www.pcworld.com/article/135293/article.html

Dhamija, R., Tygar, J. & Hearst, M., 2006. Why Phishing Works. *Proceeding of CHI-2006: Conference on Human Factors in Computing Systems.*

Dunlop, M., Groat, S. & Shelly, D., 2010. GoldPhish: Using Images for Content-Based. *The Fifth International Conference on Internet Monitoring and Protection.*

Egelman, S., Cranor, L. F. & Hong, J., 2008. You've Been Warned: An Empirical Study of the. *You've Been Warned: An Empirical Study of the, Published in Proceeding CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Pages 1065-1074* , pp. 1065-1074.

Elsevier Advanced Technology, 2015. IBM uncovers major bank fraud. *Computer Fraud and Security.*

EMC, 2014. *Phishing 2013: A Look Back,* Hopkinton: EMC.

Garfinkel, S. et al., 2005. How to make secure e-mail easier to user. *Proceedings of the ACM Conference on Human Factors in Computing Systems,* pp. 701-10.

Huang, C.-Y., Ma, S.-P. & Chen, K.-T., 2011. Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications 34,* pp. 1292-1301.

Kirda, E. & Kruegel, C., 2005. Protecting users against phishing attacks with antiphish. *Proceedings of the 29th Annual International Conference on Computer Software and Applications,* pp. 517-24.

Kumaraguru, P. et al., 2009. School of phish: a real-world evaluation of anti-phishing training",. *Proceedings of the 5th Symposium on Usable Privacy and Security.*

Kumaraguru, P. et al., 2007. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *Conference Proceeding Human-Computer Interaction Institute.*

Kumaraguru, P. et al., 2007. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* , pp. 70-81.

Kumaraguru, P. et al., 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology Vol.10 No.2.*

Malik, H. & Malik, A. S., 2011. Towards

Identifying the Challenges Associated with Emerging Large Scale Social Networks. *Procedia Computer Science*, p. 458–465.

McQuade, S. C., 2009. CyberCrime. Dalam: *Encyclopedia of cybercrime*. Westport: Greenwood Publishing Group, Inc., p. 44.

Meulen, N. S. v. d., 2013. You've been warned: Consumer liability in Internet. *Computer Law & Security Review Volume 29, Issue 6, December 2013*, p. 713–718.

Mohammad, R. M., Thabtah, F. & McCluskey, L., 2015. Tutorial and Critical analysis of phishing websites methods. *Computer science review*.

N. P. Singh, P., 2007. Online Frauds in Banks with Phishing. *Journal of Internet Banking and Commerce*, p. 4.

Nasution, S. M., 2016. *Phishing sebagai Ancaman pada Layanan Online Banking* [Wawancara] (21 January 2016).

Nilsson, M., Adams, A. & Herd, S., 2006. Building security and trust in online banking. *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*, pp. 1701-4.

Parmar, B., 2012. Protecting against spear-phishing. *Computer Fraud and Security*.

Ramzan, Z., 2010. Phishing attacks and countermeasures. *In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security, Springer. ISBN 9783642041174.*.

Ridley, D., 2012. *The Literature A Step-by-Step Guide.* London: Sage Publication.

Rush, H., Smith, C., Mbula, E. K. & Tang, P., 2009. Crime online. *Cybercrime and illegal innovation*, p. 11.

Sein, E., 2011. The God of Phishing. *Info Security Spotlight.*

Silic, M. & Back, A., 2016. The dark side of social networking sites:Understanding phishing risks. *Computers in Human Behavior*, pp. 35-43.

Symantec Brightmail TM, 2014. Anti Phishing, White Paper: Messaging Security.

Tanujaya, A., 2015. *Gameover Zeus dengan LoadInjectScript.* [Online] Available at: http://www.vaksin.com/0614-goz-load_inject_script

USE Act, 2010. Golden hour for phishing and new Zeus botnet. *Network Security*.

Vishwanath, A. et al., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems 51*, pp. 576-586.

Whittaker, C., Ryner, B. & Nazif, M., 2010. Large-Scale Automatic Classification of Phishing Pages. *Large-Scale Automatic Classification of Phishing Pages.*

Zielinska, O. A., Welk, A. K., Mayhorn, C.

. B. & Murphy-Hill, E., 2015. Exploring Expert and Novice Mental Models of Phishing. *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting.*