ISSN 2828-285x

IPB University
Bogor Indonesia
Direktorat
Kajian Strategis
dan Reputasi Akademik

PERTANIAN, KELAUTAN, DAN BIOSAINS TROPIKA
Vol. 5 No. 2 Tahun 2023

Perlindungan Konsumen terhadap Bahaya Phishing Data Perbankan

Penulis
Megawati Simanjuntak[1], Anna Maria Tri Anggraini[2]

1 Departemen Ilmu Keluarga dan Konsumen, Fakultas Ekologi Manusia, IPB University
2 Badan Perlindungan Konsumen Nasional (BPKN)

Ringkasan

Isu Kunci

Policy Brief ini memuat poin-poin penting sebagai berikut :
(a) Jasa pembayaran menjadi target utama dari kegiatan *phishing.*
(b) Indonesia menjadi urutan ke-3 dalam jumlah kasus kebocoran data terbanyak di dunia.
(c) Upaya lembaga terkait dalam menangani kasus *phishing*.

Rekomendasi

Otoritas Jasa Keuangan (OJK) harus mendorong pelaku usaha jasa keuangan untuk memperkuat sistem keamanan data nasabah yang andal, aman, dan bertanggung jawab dalam upaya mencegah dan menghentikan berbagai kasus phising. Selain itu, OJK harus membuat pedoman yang menyampaikan informasi terbaru tentang jenis dan teknik penipuan digital terbaru. Pedoman ini juga harus menjelaskan bagaimana pelaporan dilakukan kepada otoritas berwenang. Secara nasional, OJK harus menetapkan kebijakan untuk mengubah sistem verifikasi. Keempat, perlu mendorong Penyelenggara Sistem Elektronik (PSE), termasuk sektor jasa keuangan, untuk melakukan pelatihan dan melakukan evaluasi tentang seberapa efektifnya. OJK harus melakukan sosialisasi lebih luas dan terintegrasi. Keenam, Kementerian Komunikasi dan Informatika bertanggung jawab untuk mendorong pembentukan dan pembentukan lembaga yang akan bertanggung jawab atas pelaksanaan Undang-Undang. Selain itu, Kementerian harus mengawasi penyedia layanan media digital dalam menyediakan lencana verifikasi.

Perlindungan Konsumen terhadap Bahaya *Phishing* Data Perbankan

Pendahuluan

Perkembangan teknologi dalam sistem pembayaran telah menggantikan peran uang tunai sebagai alat pembayaran sehingga transaksi nontunai di Indonesia semakin efisien. Hal ini diperkuat dengan transaksi nontunai yang semakin diminati dengan hadirnya *Quick Response Code Indonesian Standard* (QRIS). Dalam dunia perbankan, salah satu bentuk penerapan teknologi informasi adalah *electronic banking* (*e-banking*). Berdasarkan Pasal 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, setiap bank berkewajiban untuk mengelola setiap jasa keuangan yang ditawarkan kepada nasabah dengan prinsip kehati-hatian yang tinggi.

Perkembangan teknologi diikuti juga berkembangnya berbagai modus operandi dalam dunia perbankan. Salah satu serangan terhadap *electronic banking* adalah *phishing*. Ancaman tersebut mendorong seseorang mengikuti tautan situs web dan memasukkan data kredensial atau mengunduh *malware* untuk melakukan peretasan (Griffiths 2023). Berdasarkan data Otoritas Jasa Keuangan (OJK) setidaknya ada 3 (tiga) kejahatan digital yang paling sering terjadi antara lain *card skimming*, *phishing*, dan *carding.* Menurut Wibowo dan Fatimah (2017) cara kerja *phishing* diantaranya *e-mail phishing, website phishing*, dan *malware phishing. Phising* merupakan bentuk rekayasa sosial yang sangat berbahaya bertujuan menipu sehingga korban mengungkapkan informasi pribadi/rahasia (Ferreira dan Teles 2019).

Data National Cyber Security Index (NCSI), indeks keamanan siber Indonesia menerima skor 38,96 poin dari 100 pada 2022. Di antara negara-negara G20, angka ini menempatkan Indonesia di peringkat ketiga terendah. Secara global, Indonesia menduduki peringkat ke-84 dari 160 negara. Interpol Cyber Assessment Report menunjukkan 2,7 juta serangan ransomware yang terdeteksi di Asia Tenggara dari Januari hingga September 2020. Indonesia di peringkat teratas dengan 1,3 juta serangan (Data Books 2022). Salah satu alasan mengapa Indonesia sangat rentan terhadap serangan siber adalah karena jaringan dan infrastruktur keamanan jaringan yang sudah tua dan sudah ketinggalan zaman tidak lagi mampu memenuhi kebutuhan operasi modern. Mencegah ancaman adaptif yang sangat mengevasive (HEAT) adalah salah satu contohnya.

Menurut data laporan Direktorat Tindak Pidana Siber Bareskrim Polri (2022), ada 5.579 serangan *phishing* terjadi di Indonesia sepanjang kuartal II tahun 2022. Jumlah serangan *phishing* ini meningkat sekitar 41,52 persen dari kuartal I tahun 2022, yaitu sebanyak 3.942 serangan. Dari sejumlah produk perbankan atau lembaga keuangan, *e-wallet d*an rekening bank dinilai sebagai produk yang rentan mengalami kebocoran data.

Indonesia memiliki hukum siber yang sangat ketat. Pasal 27 hingga 37 UU Informasi dan Transaksi Elektronik (UU ITE) mengatur klasifikasi kejahatan siber, dan Pasal 35 memberikan alasan bagi penegak hukum untuk memberikan hukuman kepada pelaku phishing. Setiap orang yang dengan sengaja mengubah, menciptakan, mengubah, menghilangkan, atau merusak informasi elektronik dan/atau dokumen elektronik dengan tujuan informasi elektronik dan/atau dokumen elektronik tersebut dianggap sebagai data asli.

Industri jasa pembayaran adalah target utama phishing. Melihat bank sebagai agen kepercayaan adalah penting untuk melindungi nasabah secara hukum. Menurut Pasal 37 butir b UU Nomor 10 Tahun 1998 tentang Perubahan Atas

UU Nomor 7 Tahun 1992 tentang Perbankan, bank harus menjamin dana masyarakat. Prinsip kerahasiaan juga mendasari kewajiban bank untuk memperhatikan kepentingan nasabahnya. Menurut prinsip ini, bank harus merahasiakan semua informasi dan data pelanggan, termasuk informasi keuangan dan pribadi.

Gambaran Kejahatan *Phising* di Indonesia

Berdasarkan data Badan Siber dan Sandi Negara (BSSN), 16.882 kasus email phishing terjadi sepanjang tahun 2022. Sektor keuangan adalah yang paling sering terkena serangan siber di seluruh dunia. Serangan siber untuk membobol bank menggunakan social engineering, OTP Fraud, SIM swap, dan phishing.

Sepanjang tahun 2021 dan 2022, BPKN-RI menerima 15 pengaduan mengenai kasus *phishing* sebanyak 15 pengaduan. Terdapat 3 (tiga) materi pengaduan terbanyak antara lain keluhan terhadap pengaduan pendebetan dana di rekening yang tidak dilakukan oleh nasabah, uang nasabah hilang di rekening serta transaksi *fraud.* Bahkan *phishing* juga menjadi salah satu prediksi ancaman siber pada tahun 2023.

Pada awalnya, metode yang paling umum adalah melalui telepon dengan nama institusi tertentu (Alkhalil et al. 2021). Menurut penelitian media, ada beberapa contoh kasus phishing: di tahun 2019, salah satu nasabah bank mengaku mendapat telepon dari seseorang yang mengaku sebagai pegawai bank, dan di tahun 2022, seorang nasabah menjadi korban kejahatan siber dengan modus link phishing hingga kehilangan uang senilai Rp1,114 miliar (Putra 2022).

Direktorat Tindak Pidana Siber Bareskrim Polri membongkar komplotan penipuan *online* yang menguras 493 rekening nasabah bank. Kerugian ditaksir mencapai dua belas miliar rupiah. Sebanyak 13 tersangka penipuan *link phishing* telah ditangkap. Modifikasi baru digunakan oleh kelompok ini untuk menyebarkan link dan modifikasi Android Package Kit (APK) yang tidak sah. Modifikasi ini disebut sebagai APK pengiriman paket, Facebook Lite, dan produk perbankan.

Strategi Pemerintah dalam Menangani *Phishing*

Kominfo senantiasa berupaya melakukan edukasi literasi digital kepada masyarakat karena kebiasaan masyarakat yang berbanding lurus dengan pelaku kejahatan. Salah satu cara terbaik untuk mencegah phishing adalah dengan mendidik pengguna (Mohammad *et al*. 2015). Kominfo juga telah bergabung dalam tim SWI (Satgas Waspada Investasi) dan juga membuka tempat pengaduan untuk menindaklanjuti terkait kasus-kasus tersebut.

Dalam hal ini, tugas BSSN adalah melakukan pemantauan. BSSN juga menyelenggarakan pengawasan terhadap sistem elektronik dan menyelenggarakan literasi keamanan siber untuk masyarakat. Saat ini BSSN telah membuat teknologi sederhana seperti mengembangkan deteksi *link* palsu menggunakan AI serta mengembangkan *password management*. Dari sisi penyelenggara sistem elektronik (PSE) juga memiliki tugas tersendiri, dua tugas dari PSE, yaitu dari sisi pengamanan dan sisi edukasi. Bank sebagai penyelenggara sistem elektronik memiliki tugas mengedukasi nasabahnya.

OJK telah mengatur mengenai seluruh resiko manajemen risiko IT ada edaran SE mengenai *cybersecurity* yang secara eksplisit *requirement* perlu dijalankan oleh nasabah. OJK juga memiliki situs yaitu kontak 157 atau website ojk.go.id untuk menambah informasi terkait permasalahan konsumen.

Bareskrim tidak berkaitan dengan proses edukasi secara spesifik karena lebih berfokus kepada tindakan moril. Konsumen harus lebih berhati-hati menggunakan media sosial dan menjaga data pribadinya terutama data perbankan, seperti PIN, *password*, dan OTP. *Phishing* sering kali

menjadi serangan masuk dengan penjahat media sosial yang mengumpulkan informasi sensitif (seperti detail *login* atau nomor kartu kredit) yang kemudian dapat digunakan untuk melancarkan serangan lebih lanjut. Sangat penting bagi pengguna untuk selalu waspada dalam menerima email dan pesan teks. Selain itu, dalam menerima panggilan mencurigakan yang meminta informasi sensitif seperti nomor rekening bank atau kata sandi. Beberapa pencegahan yang bisa dilakukan antara lain mengecek keaslian sumber informasi dan memastikan bahwa website yang dikunjungi adalah website resmi bank (Fikri *et al.* 2023).

Pihak bank sebagai "penjaga" dana nasabah juga memiliki tugas memberikan edukasi kepada nasabahnya mengenai kerahasiaan data pribadi nasabah agar tidak sembarangan diberikan kepada oknum yang mengaku sebagai wakil dari bank. Di samping itu, edukasi mengenai keamanan siber disarankan untuk diberikan sejak dini melalui kurikulum yang diajarkan di sekolah dan prosesnya melibatkan para pemuka agama. Hal ini bertujuan agar kalangan masyarakat khususnya masyarakat bawah/*grass root* dapat lebih memahami dampak keterbukaan informasi di era digital ini. Selanjutnya, kebijakan nasional perlu mereduksi sifat anonim di media sosial menjadi seminimal mungkin sehingga semua menjadi identitas yang jelas. Hal tersebut akan berdampak pada peningkatan *self responsibility* dalam ruang siber. Tentu saja tidak mudah mendorong masyarakat untuk menggunakan *password manager* sehingga membutuhkan peran banyak pihak untuk bisa bersama-sama melawan kejahatan *phishing*.

Implikasi dan Rekomendasi

Kemudahan teknologi internet dalam jasa pembayaran saat ini banyak menimbulkan permasalahan terkait keamanan di dunia perbankan. *Phishing* merupakan salah satu serangan yang terjadi pada *electronic banking.* Kasus *phishing* yang terjadi di Indonesia semakin tinggi karena internet perbankan nasional yang belum aman dari pembobolan. Oleh karena itu, lembaga terkait perlu memberantas kasus *phishing* tersebut. Cara yang dapat dilakukan lembaga terkait yaitu dengan memberikan edukasi kepada masyarakat.

BPKN-RI merekomendasikan beberapa hal yang dapat menjadi pertimbangan bagi Otoritas Jasa Keuangan dan Kementerian Komunikasi dan Informatika dalam upaya mengembangkan perlindungan konsumen berdasarkan UUPK. OJK dalam hal ini perlu mendorong pelaku usaha jasa keuangan untuk meningkatkan keamanan data nasabah, menyusun panduan informasi dan mekanisme pelaporan terkait penipuan digital, mengubah kebijakan terkait sistem verifikasi, mendorong Penyelenggara Sistem Elektronik (PSE) termasuk sektor jasa keuangan untuk memberikan edukasi, melakukan sosialisasi mengenai pentingnya menjaga kerahasiaan data pribadi. Kemudian, Kementerian Komunikasi dan Informatika perlu mempercepat pembentukan serta penetapan lembaga yang menjadi pelaksana UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP) serta peraturan turunannya, melakukan pengawasan kepada penyedia layanan media digital dalam rangka menyerahkan lencana verifikasi, meningkatkan sosialisasi literasi digital, dan melakukan kajian mengenai kebijakan SIM card berbayar.

Daftar Pustaka

Alkhalil Z, Hewage C, Nawaf L, Khan I. 2021. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060

Data Books. 2022. Indonesia alami kasus serangan ransomware terbanyak di asia tenggara [Internet]. [diakses 2023 Juni 2]. Tersedia pada https://databoks.katadata.co.id/datapublish/2022/06/08/indonesia-alami-kasus-serangan-ransomware-terbanyak-di-asia-tenggara

Ferreira A, Teles S. 2019. Persuasion: How phishing emails can influence users and bypass security measures. *Int. J. Hum. Comput. Stud.* 125:19–31.doi:10.1016/j.ijhcs.2018.12.004.

Fikri AWN, Fauzi A, Rachman AA, Khaerunisa A, Sari DP, Vernanda P, Hikmah R, Fadyanti TP. 2023. Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. *J Ilmu Multidisiplin*. 2(1):84–91.

Griffiths C. 2023. The latest 2023 cyber crime statistics (updated May 2023). *aag-it.com*. Internet. [diakses 2023 Mei 12]. https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Phishing remains the most common,1 in 5 internet users.

Kejahatan. Kejahatan perbankan digital: Lindungi datamu, amankan uangmu. Sikapi uangmu.ojk.go.id. [diakses 2023 Juni 2]. Tersedia pada https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/20661

Mohammad RM, 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

[NCSI] National Cyber Security Indeks. 2020. [diakses 2023 Juni 2]. Tersedia pada https://ncsi.ega.ee/ncsi-index/

Putra MDDB. 2022 Juni 9. Pasca nasabah kena *phising*, bri lakukan investigasi yang mengakibatkan kerugian rp1,114 miliar. HarianHaluan.com. [diakses 2023 Juni 2]. Tersedia pada https://www.harianhaluan.com/news/pr-103583285/pasca-nasabah-kena-*phising*-bri-lakukan-investigasi-yang-mengakibatkan-kerugian-rp1114-miliar

Wibowo MH, Fatimah N. 2017. Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT (Jurnal of Education and Information Communication Technology)*. 1(1): 1-2.

Policy Brief Pertanian, Kelautan, dan Biosains Tropika merupakan upaya mengantarmukakan sains dan kebijakan (science-policy interface) untuk mendukung pembangunan berkelanjutan yang inklusif. Media ini dikelola oleh Direktorat Kajian Strategis dan Reputasi Akademik (D-KASRA) IPB University. Substansi policy brief menjadi tanggung jawab penulis sepenuhnya dan tidak mewakili pandangan IPB University.

Author Profile

Megawati Simanjuntak, merupakan Dosen di Departemen Ilmu Keluarga dan Konsumen, IPB University dan pernah menjadi Komisioner di Badan Perlindungan Konsumen Nasional RI. Aktif dalam kegiatan pemberdayaan konsumen dengan area penelitian di bidang perilaku konsumen dan perlindungan konsumen. (***Corresponding Author***)
mega_juntak@apps.ipb.ac.id

Anna Maria Tri Anggraini, merupakan Komisioner di Badan Perlindungan Konsumen Nasional RI (BPKN-RI)

ISSN 2828-285X

Telepon
+62 813 8875 4005

Email
dkasra@apps.ipb.ac.id

Alamat
Gedung LSI Lt. 1
Jl. Kamper Kampus IPB Dramaga
Bogor - Indonesia 16680