Volume 2 Number 1 (2024)
January-June 2024
Page: 23 - 34

E-ISSN: 2987-095X
DOI: 10.37680/J SHEL

JSHEL
Journal of Sharia Economic Law

Mini Research Teknologi Keuangan Syariah Identitas Digital Vs Kejahatan Siber (Studi Intensitas Kasus Dan Pola Kejahatan Siber Melalui Platform Digital)

Rizka Oktafiani[1], Shela Enindra Trisnawati[2], Siti Maymunah[3], Siti Paridah[4]
[1] Institut Agama Islam Negeri, Ponorogo, Indonesia; Oktafiani08@gmail.com
[2] Institut Agama Islam Negeri, Ponorogo, Indonesia; Shela_e@gmail.com
[3] Institut Agama Islam Negeri, Ponorogo, Indonesia; Sitimaymunah@gmail.com
[4] Institut Agama Islam Negeri, Ponorogo, Indonesia; Sitiparidah80@gmail.com

Received: 09/03/2024 Revised: 15/04/2024 Accepted: 23/06/2024

Abstract

This study aims to analyze digital identity and cybercrime patterns on various digital platforms. A digital identity is a digital version of a physical identity document as well as a credential that allows a person to access online services. Cybercrime is an unlawful act committed by someone with a computer network. The method used is Descriptive Qualitative research with a Statute Approach approach through legal rules in the implementation and supervision regulated in the Legislation. While the data used are secondary data obtained from library materials, books, research literature, previous research, and internet media. The result of this study is that it can find out the number of cyber cases in the form of phishing crimes that occurred in the 2018-2021 period. This crime case peaked in 2021 due to: 1) The number of new users who understand technology so that a new identity has emerged in the use of internet media. 2) The development of mass media on several platforms with all its advantages makes thinking in the mass media less and even not balanced with the rise of cybercrime.

Keywords *Digital identity; cybercrime; phishing*

Corresponding Author
Rizka Oktafiani
Institut Agama Islam Negeri, Ponorogo, Indonesia; Oktafiani08@gmail.com

1. PENDAHULUAN

Identitas merupakan refleksi diri seseorang yang mengidentifikasi betapa berbedanya perilaku dan tingkah lakunya. Identitas merupakan ciri unik yang membedakan seseorang dengan orang lain. Tidak ada seorang pun yang mempunyai identitas yang sama. Sedangkan Digital adalah teknologi yang mampu menyimpan, membuat, dan memproses berbagai jenis data suatu individu atau kelompok. Jadi pengertian identitas digital adalah segala jenis informasi atau data yang ada di dunia maya, terhubung dengan orang, organisasi, atau bahkan perangkat elektronik tertentu, yang ditandai dengan rangkaian kode unik atau nama pengguna tertentu. (Nafi'ah, 2020)

Identitas digital adalah versi digital dari dokumen identitas fisik dan juga kredensial yang memungkinkan seseorang mengakses layanan online. Tujuan utama dari identitas digital adalah untuk menciptakan tingkat kepercayaan yang sama seperti dalam transaksi atau interaksi tatap muka

yang sebenarnya. Di era digital, transaksi digital menjadi hal yang tidak bisa dihindari. Setiap interaksi memerlukan landasan rasa saling percaya dari masing-masing pihak. Salah satunya adalah bentuk kejahatan dunia maya *(cybercrime)*.

Kejahatan dunia maya adalah salah satu bentuk kejahatan virtual penggunaan sumber daya komputer terhubung ke internet dan mendapat manfaat komputer lain yang terhubung ke Internet juga. Ada celah keamanan dalam sistem operasi menyebabkan kelemahan dan keterbukaan celah yang bisa dieksploitasi oleh peretas. Maka dapat di simpulkan bahwa *cybercrime* adalah tindak melawan hukum yang dilakukan seseorang dengan jaringan komputer dengan tujuan memperoleh keuntungan atau tidak yang tentunya tetap merugikan salah satu pihak. (Apriwandi, 2022)

Cybercrime merupakan kejahatan yang tak akan pudar oleh waktu. Hal itulah yang harus menjadikan kewaspadaan pada pemilik perusahaan untuk mampu memberikan layanan yang menjamin keamanan data penggunanya. Perusahaan harus mampu bekerja sama dengan pemerintah untuk semakin mengurangi dampak negatif adanya *cybercrime* dinegaranya. Contohnya yaitu kasus peretasan pada bank syariah.

Kasus peretasan yang terjadi pada bank BSI baru-baru ini harus menjadi pertimbangan lain oleh para perusahaan bagaimana memberi keaman pada data setiap pelanggannya. Beberapa narasumber memberikan keterangan bahwasannya peretasan tersebut mungkin dilakukan sejak libur lebaran dan berakibat nasabah dengan transaksi yang tidak wajar akan terekspos dan tentunya akan menjadi perhatian publik. Kasus seperti ini tentu menyiratkan bahwa sistem keamanan BSI yang sangat lemah. (Kontan co.id, 2023)

Perusahaan hendaknya mampu menjamin keamanan data dari setiap bagian yang ada dalam perusahaan tersebut seperti karyawan maupun nasabahnya. Pada undang-undang (UU) No. 27 tahun 2022 efektif 17 Oktober 2022 mengenai perlindungan data pribadi jelas disebutkan bahwa perlindungan tersebut menjamin warga akan perlindungan diri pribadi dan pentingnya hal tesebut. Dalam peraturan OJK No. 11/POJK.03/2022 menjelaskan tentang harus adanya pusat pemulihan bencana yang tentu digunakan untuk memulihkan lagi data data yang terganggu atau rusak. Bank hendaknya memiliki komite pengarah teknologi informasi yang memberikan tanggung jawab penuh memberikan saran dan pertimbangan untuk menyelesaikan permasalah terkait dengan teknologi dan informasi. (Sutarli, 2023)

Sedangkan pada tahun 2020, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) mencatat 2549 kejadian peretasan di Indonesia menggunakan email phising. Peningkatan email *phishing* terbesar terjadi pada kuartal kedua tahun lalu, tepatnya pada bulan Maret hingga Mei 2020 dan jumlah kasus tertinggi terjadi pada jam kerja. Phishing adalah metode penipuan sehingga penipu dapat memperoleh informasi rincian beberapa akun secara ilegal. Kata lain dari *phishing* adalah

pengambilan kata sandi, yang berarti kejahatan mencoba mengambil suatu data. Penipuan ini menipu pengguna untuk memasukkan data akun seperti nama pengguna dan kata sandi ke situs web palsu *(spoof website)*. (Cnbc Indonesia, 2021)

Sehingga dalam menanggulangi phising di Indonesia dapat dilihat dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) penting dalam memerangi penipuan di Indonesia. UU PDP menjamin perlindungan data pribadi seseorang dan memberikan hukuman berat bagi pelaku kejahatan dunia maya, termasuk pelaku Phising. Merupakan tanggung jawab pemerintah untuk memastikan ketentuan UU PDP diterapkan dan dipatuhi dengan baik untuk melindungi data pribadi masyarakat. (Sutarli, 2023)

Analisis kejahatan *cyber* dapat menambah kewaspadaan pengguna media sosial baik di kalangan individu, organisasi, dan masyarakat pada umumnya. Terutama dalam memberikan informasi identitas pribadi melalui berbagai platform digital. Dan juga dapat mendukung dalam mengembangkan kebijakan keamanan *Cyber*, dengan memahami mengenai ancaman dan tantangan yang akan dialami dan berkembang didunia *Cyber*. Usaha tersebut dapat dilakukan engan cara mengembangkan alat dan metode baru dalam mendeteksi, mencegah, dan mencegah serangan *Cyber* itu sendiri. Dengan adanya peningkatan keamanan *Cyber* dapat meningkatkan kepercayaan publik terhadap layanan digital. Dengan adanya peningkatan perlindungan terhadap data pribadi dan informasi sensitif, tentunya masyarakat akan merasa lebih aman dan percaya dalam menggunakan teknologi digital.

2. METODE

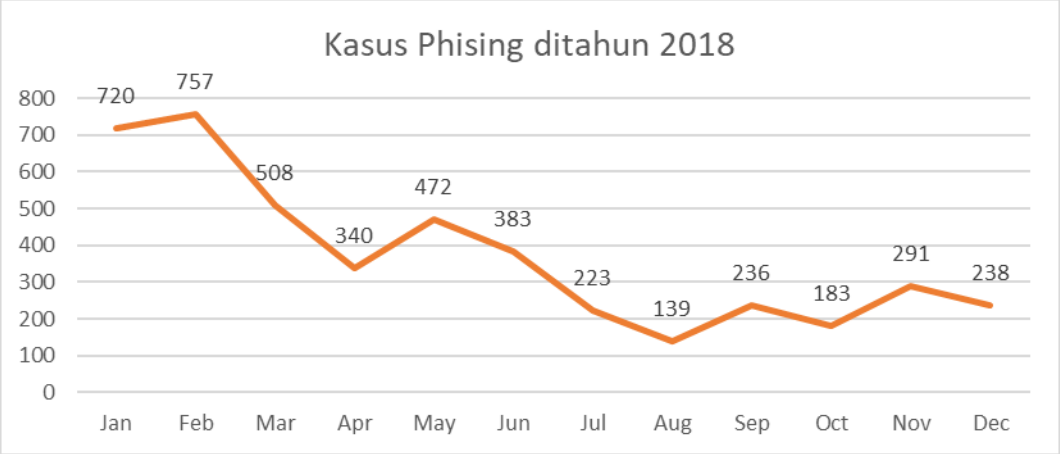
Penelitian ini menggunakan penelitian kualitatif deskriptif. Pendekatan kualitatif adalah jenis penelitian yang temuan-temuannya tidak diperoleh melalui prosedur statistik atau bentuk hitungan lainnya dan bertujuan mengungkapkan gejala secara holistik kontekstual melalui pengumpulan data dari literatur dan jurnal-jurnal penelitian dengan memanfaatkan diri penulis sebagai instrumen kunci. Sedangkan pendekatan deskriptif adalah penelitian yang dimaksudkan untuk menyelidiki keadaan, kondisi atau hal lain-lain yang sudah disebutkan, yang hasilnya dipaparkan dalam bentuk laporan penelitian. Penelitian ini juga menggunakan pendekatan perundang-undangan atau *Statute Approach*. Pendekatan *Statute Approach* digunakan karena penelitian berhubungan dengan aturan hukum dalam pelaksanaan dan pengawasan yang diatur dalam Perundang- undangan.

Dalam pengumpulan data, sumber data yang digunakan adalah Data Sekunder. Data Sekunder yaitu data yang didapatkan oleh orang yang melakukan penelitian dan diambil dari data-data yang sudah ada. Data sekunder diperoleh dari bahan pustaka, buku, literatur penelitian, penelitian terdahulu, dan media internet. Pada metode ini peneliti akan menyampaikan mengenai analisis

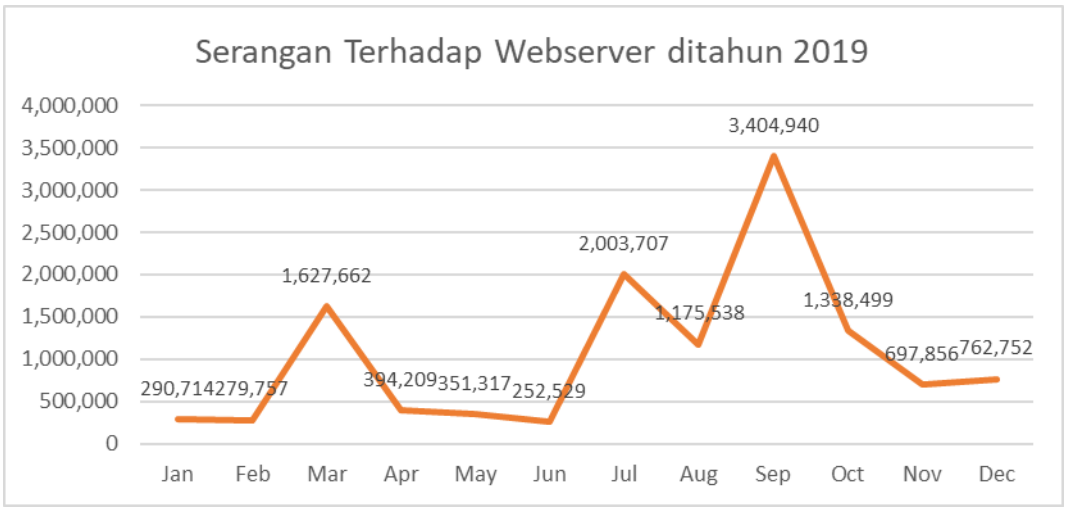
sebagaimana penggunaan analisis kualitatif. Langkah akhir pada analisis penelitian kualitatif yaitu pengambilan kesimpulan.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil dari pengumpulan data melalui BSSN (Badan Siber dan Sandi Negara) dapat diketahui jumlah kasus *phising* yang terjadi beberapa tahun lalu:

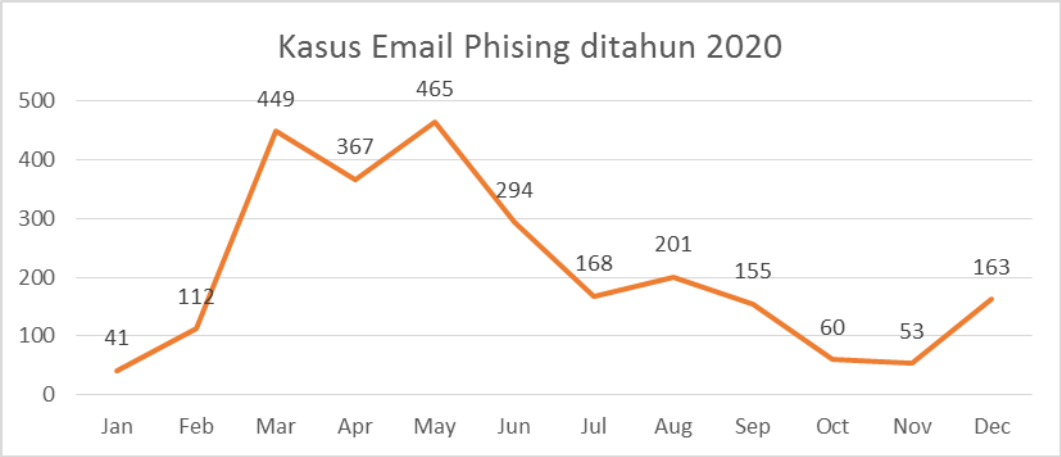


Dari data tersebut dapat menunjukkan sejumlah kasus yang terjadi dalam periode tersebut. Terdapat sejumlah situs yang diketahui menyamarkan, memalsukan, dan membuat situs yang semirip mungkin dengan aslinya. Terdapat 4.499 tautan *phising* yang disebar luaskan dengan 1.654 web yang berdomain indonesia yang terkena atau terindikasi melakukan *phising*. Dan 2.845 lainnya merupakan web yang berdomain Internasional. (Bssn, 2018)

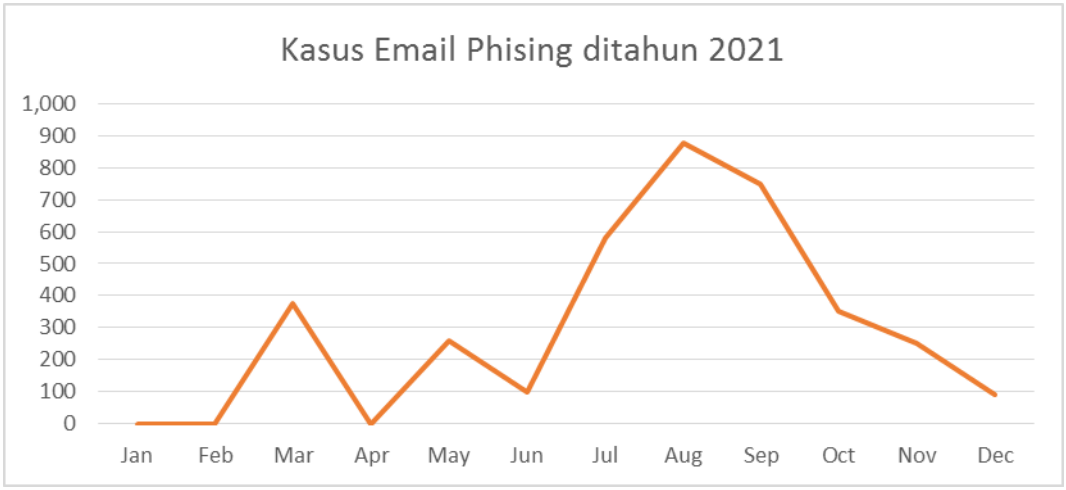


Serangan cyber terus melonjak tajam pada bulan September hingga Oktober, dan mengalami penurunan yang sangat drastis pada bulan November. Banyaknya serangan ini bertepatan dengan pelantikan presiden dan wakilnya periode 2019-2024. Diketahui total serangan tersebut berjumlah 12,579,480 terhadap web server yang didalamnya termasuk pengubahan tampilan, *phising*, dan infeksi

malware. (Bssn, 2019)



Pada tahun 2020, Pusopskamsinas mendeteksi kasus email *phising* sebanyak 2.549 kasus. Puncak tertinggi email *phising* terjuadi pada bulan Maret hingga Mei secara signifikan. Diketahui juga sebanyak 55,53% email *phising* disebar pada jam kerja (09.00 – 17.00) dan sisanya yang berjumlah 44,37% terkirim pada jam diluar kerja (17-00 – 09.00). (Bssn, 2020)



Tercatat bahwasannya kasus email *phising* yang terjadi di tahun 2021 sebanyak 3.816 kasus dengan pelonjakan tajam terjadi dibulan Agustus. Diketahui bahwa 53% email phising terkirim pada jam kerja dan 47% diluar jam kerja. (Adi, 2021)

3.1. Kasus *Phising* ditahun 2018

Phishing adalah metode penipuan sehingga penipu dapat memperoleh informasi rincian beberapa akun secara ilegal berupa pengambilan kata sandi, yang berarti kejahatan untuk mengambil suatu informasi data pribadi seseorang melalui internet. Pada tahun 2018 kasus *phising* berjumlah 4.499 tautan *phising* yang disebar luaskan dengan 1.654 web yang berdomain indonesia yang terkena atau terindikasi melakukan *phising*. Dan 2.845 lainnya merupakan web yang berdomain internasional. Lonjakan paling tinggi terjadi pada awal bulan Januari dan Februari yang disebabkan adanya tren saluran penyampaian konten baru. (Latifahi, 2022)

Tahun 2018 menunjukkan bahwa penjahat dunia maya memantau dengan cermat peristiwa-peristiwa global dan menggunakannya untuk mencapai tujuan mereka. Kami telah melihat peningkatan yang stabil dalam serangan *phishing* yang menargetkan sumber daya terkait mata uang kripto, dan kami memperkirakan penipuan baru akan muncul pada tahun 2019. Meskipun terjadi kehilangan nilai dan masa-masa sulit di pasar kripto, *phisher* dan *spammer* masih berusaha mencuri apa pun yang mereka bisa. Pada tahun terakhir juga menunjukkan bahwa pelaku spam dan penipu terus mengeksploitasi acara tahunan seperti peluncuran ponsel cerdas baru, musim penjualan, dan tenggat waktu pajak serta keringanan pajak. (Securelist, 2019)

Selain itu pada tahun ini, penjahat dunia maya menggunakan cara-cara baru untuk berkomunikasi dengan "audiens" mereka, seperti pesan instan dan jejaring sosial, untuk menyebarkan pesan jahat satu demi satu, dan seterusnya. Pesan menyebar secara independen satu sama lain. Sehingga seperti yang ditunjukkan oleh serangan terhadap universitas, penipu tidak hanya mencari cara baru, tetapi juga target baru.

3.2. Serangan Terhadap Webserver ditahun 2019

Pada tahun 2019 dunia siber diramaikan dengan dua peristiwa besar. Insiden pertama melibatkan insiden siber yang terus-menerus menyerang sistem keamanan siber nasional, dan insiden kedua melibatkan upaya pemerintah untuk memperkuat keamanan siber nasional. Serangan siber tidak harus dilakukan dari sumber serangan yang terdaftar, namun bisa berasal dari negara lain dengan menggunakan negara asal serangan sebagai pijakan atau platform. Seperti sistem pengawasan nasional Mat Garuda BSSN menuliskan 290,3 juta serangan siber di Indonesia sepanjang tahun 2019. Serangan terbesar berasal dari alamat IP di negara Amerika Serikat, berubah dibandingkan kondisi tahun sebelumnya yang tercatat tambahan alamat IP di Indonesia sendiri. (Bssn, 2019)

Selain itu juga terdapat malware, insiden siber yang penting yaitu kebocoran data dan pemadaman listrik. Peristiwa kebocoran data antara lain kebocoran data penumpang Malindo Air, anak perusahaan Lion Air, dan kebocoran data 13 juta akun Bukalapak yang diperdagangkan di situs gelap. Pemadaman listrik *(blackout)* yang terjadi selama 9 jam pada tanggal 4 Agustus 2019 sangat berdampak pada internet dan bisnis digital yang beroperasi di dalamnya.

Ancaman siber akan terus ada dan semakin canggih. Menurut FBI, kejahatan siber yang dilakukan di Amerika Serikat sepanjang tahun 2019 menyebabkan kerugian sebesar USD 3,5 miliar atau sekitar Rs 47,9 triliun. Donna Gregory, direktur Pusat Pengaduan Kejahatan Internet FBI, mengatakan: "penjahat menjadi lebih canggih dan semakin sulit bagi korban yang ditipu untuk menentukan mana yang asli dan mana yang palsu."

Server web adalah serangkaian perangkat keras dan perangkat lunak pada server. Di sisi perangkat lunak, memiliki fungsi untuk mendukung penerimaan permintaan berupa halaman web

dalam protokol HTTP atau HTTPS. Setelah menerima permintaan, server web memuat dan mengirimkan halaman yang diminta untuk disajikan di browser pengguna, misalnya Google Chrome, Mozilla Firefox, Safari, dll. Sedangkan pada sisi *hardware*, web server terhubung ke Internet untuk bertukar informasi (data atau file) antar perangkat lain yang terhubung. Data yang dimaksud dapat berupa file HTML, gambar, file JavaScript, atau *stylesheet CSS*. Perangkat keras web server juga berfungsi untuk menyimpan *software* web server. Web server biasanya berfungsi sebagai mentransfer data, membersihkan cache, memeriksa keamanan dari permintaan HTTP.

Pada bulan Agustus hingga Desember tahun 2019 kasus serangan Webserver semakin melonjak tajam. Pada Agustus terjadi lebih dari 1.175.538 kasus dan puncaknya terjadi pada bulan September sebanyak 3.404.940 kasus. Hal ini disebabkan karena pada saat itu terjadi pelantikan presiden dan wakil presiden periode 8. Sehingga banyak masyarakat terkena dampak akan pelantikan tersebut karena pelaku kejahatan mencoba mengarahkan pengguna web server mengunjungi web palsu untuk melihat informasi pelantikan tersebut. Dengan begitu para pelaku kejahatan dapat dengan mudah untuk mencuri informasi mereka pada lokasi dan wilayah tertentu. (Bssn, 2019)

3.3. Kasus Email *Phising* ditahun 2020 dan 2021

Berdasarkan Pusat Operasi Keamanan Siber Nasional ((Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 88.414.296 serangan siber terjadi sejak 1 Januari sampai 12 April 2020. Pada bulan Januari, tercatat 25.224.811 serangan dan pada bulan Februari, tercatat 29.188.645 serangan. Terdapat 26.423.989 serangan di bulan Maret, dan 7.576.851 serangan tercatat pada 12 April 2020. Serangan terbanyak terjadi pada 12 Maret 2020 sebanyak 3.344.470 serangan. Sejak itu, jumlah serangan menurun secara signifikan seiring diterapkannya kebijakan bekerja dari rumah (WFH) di berbagai lokasi. Namun, serangan siber tersebut memanfaatkan isu terkait COVID-19 saat bekerja dari rumah.

Phishing adalah tindakan menyamar sebagai orang atau organisasi yang berwenang melalui email untuk mendapatkan akses ke informasi pribadi seperti ID pengguna, kata sandi, dan data penting lainnya. Email *phishing* juga diartikan sebagai jenis *phishing* yang biasa digunakan oleh peretas untuk mengelabui korbannya. Email *phishing* ditandai dengan hacker mengirimkan email dengan judul (subyek) yang menarik untuk menggugah rasa penasaran korbannya dan mendorongnya untuk membuka email tersebut. Email biasanya berisi lampiran atau tautan yang mengarahkan korban ke situs web tempat mereka dapat mengunduh program jahat. Setelah terinstal, program jahat ini secara otomatis berjalan di komputer korban dan mencuri kredensial login, kata sandi, akun, dan informasi sensitif lainnya. Selain itu, peretas menggunakan frasa, tipografi, karakter, dan/atau logo yang sama untuk membuat pesan tampak sah. (Adi, 2021)

Kasus kejahatan email phising berdasarkan Pusopskamsinas pada tahun 2020 berjumlah sebanyak 2.549 kasus. Puncak tertinggi email phising terjadi pada bulan Maret hingga Mei secara signifikan. Hal ini dikarenakan pada awal bulan Maret bertepatan dengan munculnya pertama kali Covid-19 di Indonesia. Sehingga pemerintah memberikan pemberitahuan untuk melakukan kegiatan yang berada diluar rumah dialihkan secara *daring* (dalam jaringan) atau media *online*. Seperti yang telah dilakukan organisasi-organisasi dan perusahaan-perusahaan dalam menyampaikan informasinya. Dengan adanya hal tersebut banyak sekali orang mencari kesempatan untuk mencuri informasi data tersebut. (Bssn, 2019)

Sedangkan selama tahun 2021, Direktorat Operasi Keamanan Siber mencatat kasus email phishing sebanyak 3.816 kasus dengan kasus tertinggi terjadi pada bulan Agustus 2021 yang terjadi pada jam kerja dan diluar jam kerja. Sebanyak 53% email *phishing* dikirim pada jam kerja (09.00 - 17.00) dan 47% dikirim di luar jam kerja (17.00-09.00). Kasus email *phishing* pada bulan Januari-Februari 2021 tidak terdeteksi dikarenakan adanya *maintenance* yang dilakukan.

Kategori yang paling umum adalah email *phishing* tipe faktur sebesar 10%, diikuti oleh email phishing tipe dokumen pengiriman sebesar 9%, dan email phishing tipe pesanan sebesar 4%. Judul email phishing di atas pasti akan menarik perhatian korbannya dan membuat mereka membuka email tersebut dan mendownload *attachment* atau mengklik link yang terdapat di email. Kategori-kategori ini hanya mewakili sebagian kecil dari total email *phishing* yang terdeteksi. Dari jumlah tersebut, 66% adalah email phishing dengan kategori tidak ditentukan. Sebagian besar judul email phishing terkait dengan keuangan, seperti permintaan faktur, pembayaran, bukti pembayaran, dan kuitansi.

Kasus tertinggi terjadi pada tahun 2021 yang berjumlah 1.637.973.022 kasus. Hal ini terjadi karena pada jam kerja dan diluar jam kerja. Sebanyak 53% email phishing dikirim pada jam kerja (09.00 - 17.00) dan 47% dikirim di luar jam kerja (17.00-09.00). Kasus email *phishing* pada bulan Januari-Februari 2021 tidak terdeteksi dikarenakan adanya *maintenance* yang dilakukan. Sedangkan pada tahun 2020, serangan siber menjadi risiko yang paling ditakuti seiring dengan semakin meluasnya aktivitas perdagangan online. Asosiasi Fintech Indonesia mengatakan risiko serangan siber terus meningkat seiring meningkatnya jumlah pengguna layanan keuangan digital di masa pandemi COVID-19. Industri keuangan yang kini mengandalkan layanan keuangan digital juga memberikan peluang terjadinya kejahatan *phishing*. (Adi, 2021)

Menanggapi kasus kejahatan siber ini memerlukan pembangunan lingkungan siber yang strategis dan pengelolaan sistem elektronik yang aman dan andal. Mempromosikan dan menumbuhkan ekonomi digital dengan memperkuat daya saing dan inovasi siber. Selain meningkatkan ketahanan nasional dan kesadaran serta kepekaan keamanan di dunia maya, pemerintah telah menerapkan Peraturan Presiden Nomor 53 Tahun 2017 dan perubahan ketentuan

tentang Pelayanan Sandi Siber Nasional (BSSN) dan Perpres Nomor 133 Tahun 2017. Misinya adalah melaksanakan keamanan siber secara efektif dan efisien melalui pemanfaatan, pengembangan, dan integrasi seluruh elemen yang terkait dengan keamanan siber nasional.

Tujuan strategis dari strategi keamanan siber Indonesia adalah untuk mencapai ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber, dan keamanan siber dalam ekonomi digital. Strategi keamanan informasi Indonesia diharapkan menjadi salah satu landasan kepercayaan global terhadap Indonesia di berbagai forum keamanan siber internasional. Strategi Keamanan Siber Indonesia merupakan kontribusi bangsa Indonesia dalam mendorong terciptanya perdamaian dunia.

4. KESIMPULAN

Cybercrime adalah tindak melawan hukum yang dilakukan seseorang dengan jaringan komputer dengan tujuan memperoleh keuntungan atau tidak yang tentunya tetap merugikan salah satu pihak. Kejahatan Cyber salah satunya yaitu *phishing*. *Phishing* adalah metode penipuan sehingga penipu dapat memperoleh informasi rincian beberapa akun secara ilegal. Berdasarkan hasil dari pengumpulan data melalui BSSN (Badan Siber dan Sandi Negara) dapat diketahui jumlah kasus *phising* yang terjadi di tahun 2018 yaitu berjumlah 4.499 tautan *phising* yang disebar luaskan dengan 1.654 web yang berdomain indonesia yang terindikasi melakukan *phising*. Dan 2.845 lainnya merupakan web yang berdomain internasional. Lonjakan paling tinggi terjadi pada awal bulan Januari dan Februari yang disebabkan adanya tren saluran penyampaian konten baru.

Sedangkan tahun 2019 pada bulan Agustus hingga Desember tahun 2019 kasus serangan Webserver semakin melonjak tajam. Pada Agustus terjadi lebih dari 1.175.538 kasus dan puncaknya terjadi pada bulan September sebanyak 3.404.940 kasus. Hal ini disebabkan karena pada saat itu terjadi pelantikan presiden dan wakil presiden periode 8. Tak berhenti sampai disitu, serangan cyber terus meningkat pada tahun 2020-2021, ketika itu serangan terbanyak terjadi pada 12 Maret 2020 sebanyak 3.344.470 serangan. Hal ini dikarenakan pada awal bulan Maret bertepatan dengan munculnya pertama kali Covid-19 di Indonesia. Sehingga pemerintah memberikan pemberitahuan untuk melakukan kegiatan yang berada diluar rumah dialihkan secara *daring* (dalam jaringan) atau media *online*.

Puncak kasus tertinggi terjadi pada tahun 2021 yang berjumlah 1.637.973.022 kasus. Hal ini terjadi karena pada jam kerja dan diluar jam kerja. Sebanyak 53% email *phishing* dikirim pada jam kerja (09.00 - 17.00) dan 47% dikirim di luar jam kerja (17.00-09.00). Kasus email phishing pada bulan Januari-Februari 2021 tidak terdeteksi dikarenakan adanya *maintenance* yang dilakukan. Jadi untuk menangani hal tersebut pemerintah menanggulanginya dengan menerapkan Peraturan Presiden

Nomor 53 Tahun 2017 dan perubahan ketentuan tentang Pelayanan Sandi Siber Nasional (BSSN) dan Perpres Nomor 133 Tahun 2017.

REFERENSI

Ananta Fadli Sutarli, Shelly Kurniawan. "*Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dan Menanggulangi Phising Di Indonesia*", Vol. 3. 2. 2023, Https://J-Innovative.Org/Index.Php/Innovative.

Apriwandi, Apriwandi, Dan Herycson Herycson. *"Cyber Crime Dan Fraud Kartu Kredit Dan Kartu Debit: Perspektif Akuntansi", Jueb : Jurnal Ekonomi Dan Bisnis* 1, No. 3 (30 September 2022): 111–24. Https://Doi.Org/10.57218/Jueb.V1i3.277.

Barama, Michael. *"Elektronik Sebagai Alat Bukti Dalam Cyber Crime"*

Cnbc Indonesia, "Kasus Phising Email Yang Serang Indonesia Makin Merajalela", 06 Maret 2021,18:03, Https://Www.Cnbcindonesia.Com/Tech/20210306162132-37-228322/Kasus-Phising-Email-Yang-Serang-Indonesia-Makin-Merajalela.

Habibi, Miftakhur Rokhman, Dan Isnatul Liviani. *"Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia"*, Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam 23, No. 2 (19 Desember 2020): 400–426. Https://Doi.Org/10.15642/Alqanun.2020.23.2.400-426.

Kontan.Co.Id, "Kasus Peretasan Data Bank Syariah Indonesia Bsi, Bareskrim Masuk Penyelidikan", 19 Mei 2023 13:15 Wib, Https://Amp.Kontan.Co.Id/News/Kasus-Peretasan-Data-Bank-Syariah-Indonesia-Bs-Bareskrim-Masuk-Proses-Penyelidikan,.

Latifahi, Fitri Nur, Imron Mawardi, Dan Bayu Wardhana. *"Threat Of Data Theft (Phishing) Amid The Trend Of Fintech Users In The Covid- 19 Pandemic (Study Of Phishing In Indonesia) Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid – 19 (Study Phishing Di Indonesia)"*, 6, No. 1 (2022).

Mustofa, Muhamad Bisri, Evin Luthfiah Dwiandrini, Indriani Agustin, M Afief Esyarito, Mutiara Anggraeni, Dan Siti Wuryan. *"Media Massa Dan Cyber Crime Di Era Society 5.0 (Tinjauan Multidisipliner)"*.

Nafi'ah, Rahmawati. *"Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce"*, Cyber Security Dan Forensik Digital 3, No. 1 (23 Juli 2020): 7–13. Https://Doi.Org/10.14421/Csecurity.2020.3.1.1980.

Nugroho Adi. *Laporan Tahunan Monitoring Keamanan Siber 2021*. Jl. Harsono Rm No.70, Rangunan, Jakarta Selatan, Dki Jakarta, Indonesia 12550: 2021, Https://Www.Bssn.Go.Id/.

Pusat Operasi Dan Keamanan Siber Nasional Badan Siber Dan Sandi Negara. "*Laporan Tahunan 2020 Monitoring Keamanan Siber:*. Jakarta Selatan 12550, Dki Jakarta , Indonesia.: 2020,

Https://Www.Bssn.Go.Id/.

Pusat Operasi Dan Keamanan Siber Nasional Badan Siber Dan Sandi Negara (BSSN). *Indonesia Cyber Security Monitoring Report 2018*. Jakarta Pusat 10340: 2018, *Https://Www.Bssn.Go.Id/*.

Indonesia Cyber Security Monitoring Report 2019, *Https://Www.Bssn.Go.Id/*.Securelist. *Spam And Phising In 2018*. 2019, 2019.