Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-11

Penipuan Penambah *Followers* Instagram: Analisis Serangan *Phising* dan Dampaknya pada Keamanan Data

Muhammad Arif Bagus Dewanto*, Muhammad Fathurrahman, Danar Restu Firdaus, Aep Setiawan

Sekolah Vokasi, IPB University

Abstrak: Penelitian ini membuktikan kerentanan terhadap keamanan siber terhadap web tipuan. Baik studi literatur maupun pemodelan mengenai web tipuan ini menjadi dasar metode dalam menghasilkan analisis penelitian dan kesimpulan. Web tipuan ini menjadi bukti jika serangan siber terjadi bukan hanya karena serangan langsung dari luar, tapi juga karena lengahnya kewaspadaan. Pada penelitian ini dibahas lebih lanjut mengenai cara kerja web tipuan, contoh pemodelan, dan bagaimana cara mencegahnya agar data kita dapat lebih aman.

Kata kunci: Data, Keamanan, Siber

DOI: https://doi.org/10.47134/pjise.v1i4.2672
*Correspondence: Muhammad Arif Bagus Dewanto
Email: arifdmuhammad@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *This research proves the vulnerability of cyber security to fraudulent websites. Both literature studies and modeling regarding this deceptive web are the basis for the method in producing research analysis and conclusions. This fraudulent website is proof that cyber-attacks occur not only because of direct attacks from outside, but also because of a lack of vigilance. In this research, we discuss further how deceptive websites work, modeling examples, and how to prevent them so that our data can be safer.*

Keywords: *Cyber, Data, Security*

Pendahuluan

Permintaan akan teknologi jaringan komputer terus meningkat. Internet tidak hanya menjadi sumber informasi, tetapi juga mendukung kegiatan komunitas komersial yang kini tumbuh paling cepat dan melintasi berbagai batas negara. Bahkan, pasar global dapat diakses 24 jam melalui jaringan ini. Dalam dunia maya atau *cyber space*, berbagai hal dapat dilakukan. Aspek positifnya tentu mendukung perkembangan teknologi global dan mendorong kreativitas manusia. Namun dampak negatifnya tidak bisa diabaikan begitu saja. Ketika pornografi menyebar secara online, masyarakat seringkali gagal mengambil tindakan terhadapnya (Ketaren, 2016).

Kejahatan dapat terjadi dimana saja, terbaru kini adalah *cyber crime* atau kejahatan siber. Kejahatan *Cyber* merupakan bentuk atau dimensi baru kejahatan modern dan telah mendapat perhatian internasional yang signifikan. Volodymyr Golubev menyebut ini sebagai bentuk baru perilaku antisosial. Kejahatan tidak dapat dianggap remeh dikarenakan sekarang hampir semua sektor menerapkan sistem digital yang menjadi ruang untuk kejahatan ini ada. Banyak cara yang harus dilakukan untuk mencegah kejahatan ini dan perlu disadari oleh masyarakat. Namun, pemerintah sendiri perlu untuk turut serta dalam menjaga atau sebagai perlindungan utama bagi masyarakat terhadap kejahatan ini (Gulo et al., 2021).

Perlu diingat bahwa interaksi masyarakat digital saat menggunakan Internet sangat bergantung pada ketersediaan, integritas, dan kerahasiaan informasi di dunia maya. Oleh karena itu, penting untuk melindungi infrastruktur negara ketika menggunakan teknologi informasi. Ancaman keamanan siber tidak lagi hanya sekedar permasalahan teknis keamanan komputer, namun juga mencakup dimensi ideologi, politik, ekonomi, sosial, budaya, dan keamanan nasional. Di tingkat internasional, negara-negara dan komunitas internasional perlu mengembangkan strategi kerja sama untuk mengatasi meningkatnya proliferasi dunia maya, termasuk menetapkan norma-norma internasional mengenai isu dan ancaman dunia maya (Chotimah, 2019).

Keamanan jaringan komputer tidak hanya mencakup satu aspek, tetapi terdiri dari empat elemen kunci: perangkat lunak , perangkat keras jaringan, layanan *Internet of Things*, dan sumber daya bersama. Menurut definisi keamanan jaringan komputer Organisasi Internasional untuk Standardisasi, keamanan jaringan komputer adalah perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer dari kerusakan, gangguan, atau kerentanan keamanan yang disebabkan oleh kecelakaan atau aktivitas jahat untuk melakukannya. Ini memastikan bahwa komputer sistem Anda berfungsi dengan andal dan Anda dapat menjalankan layanan komputer secara teratur (Munawar et al., 2020).

Phishing adalah jenis serangan siber di mana penyerang menyamar sebagai organisasi atau individu terpercaya untuk mendapatkan informasi sensitif dari korban, seperti kata sandi, nomor kartu kredit, dan informasi pribadi lainnya. Hal ini biasanya dilakukan melalui email, SMS, atau situs web palsu yang dirancang agar terlihat sah. Serangan *phishing* dapat menyebabkan kerugian finansial, pencurian identitas, dan pelanggaran data.

Oleh karena itu, kesadaran dan pendidikan tentang cara mengenali dan menghindari *phishing* sangat penting untuk melindungi diri Anda dari ancaman ini.

Phishing diatur dalam UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, pengaturannya dinilai belum jelas dan mengalami kekaburan hukum. *Phishing* pada dasarnya merupakan perbuatan membuat situs web palsu yang menyerupai situs resmi, lalu pelaku mengarahkan korban untuk mengakses situs palsu tersebut melalui email, pesan, atau tautan agar korban memasukkan informasi pribadi rahasia seperti *username*, *password*, nomor kartu kredit, dll. Informasi sensitif ini kemudian diketahui pelaku untuk digunakan secara ilegal sehingga merugikan korban. Pasal-pasal terkait seperti 35 dan 28 tidak mencakup unsur *phishing* secara utuh sebagai kesatuan tindakan manipulasi data dan penipuan, sehingga diusulkan perumusan konsep *phishing* yang jelas dan revisi Pasal 35 agar dapat menindak pelakunya dengan tepat (Budi et al., 2021).

Phishing adalah kejahatan dunia maya dan saat ini merupakan aktivitas kriminal yang tersebar luas yang dapat dilakukan dari jarak jauh melalui jaringan komputer (Wibowo & Fatimah, 2017). Serangan *phishing* adalah jenis serangan yang mengirimkan link yang mengarahkan korban ke halaman di situs web palsu. Biasanya situs-situs ini tampak dapat dipercaya dan asli. Tujuan dari teknik *phishing* ini sendiri adalah untuk mendapatkan informasi sensitif seperti email, *username*, *password*, dan data sensitif lainnya dari korban. Dengan mengeksploitasi kelemahan server dalam validasi masukan pengguna, serangan *phishing* mengeksekusi kode di browser web korban, mengubah tampilan halaman web atau mengarahkan pengguna ke halaman lain yang berisi aplikasi berbahaya. Selain itu, jenis serangan ini juga memungkinkan penyerang mencuri *cookie* pengguna lain.

(Yudha et al., 2018).

Metode

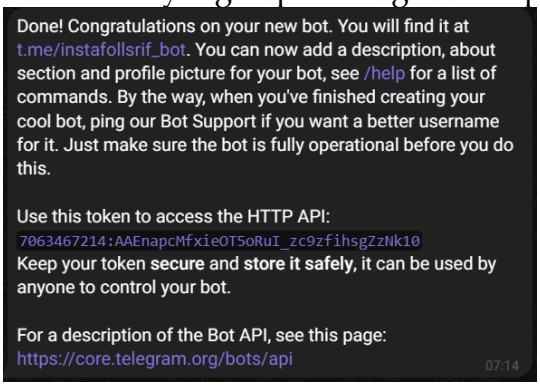
Penelitian ini menggunakan pendekatan kualitatif berdasarkan data non numerik seperti teks dan gambar. Data disaring untuk memungkinkan interpretasi dari tinjauan literatur, buku, dan artikel dari sumber yang dapat dipercaya (Islami, 2018). Dalam penelitian kali ini, penulis akan membuat sebuah *website* yang berisi *phising* mengenai Penambah *Followers* Instagram, yang mana di dalam *website* ini terdapat *login page* Instagram yang sebenarnya merupakan *login page* palsu. Jika pengguna memasukkan kredensial pengguna dan kata sandinya dalam formulir *login* (formulir *login* palsu), penjahat dunia maya dapat menganggap ini sebagai bentuk *phishing* (Kharisma Putra et al., 2023).

1. Penggunaan API BOT Telegram

Skema dari serangan ini adalah, target memasukkan *username* dan *password* dari *login page* palsu yang telah dibuat. *Username* dan *password* yang dimasukkan target kemudian dikirimkan ke Telegram si *hacker* melalui bot API Telegram. Aplikasi Telegram merupakan

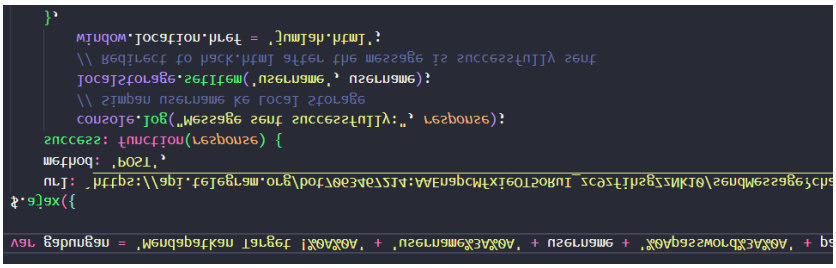
layanan pesan instan berbasis *cloud* yang memungkinkan Anda mengembangkan chatbot (Sudiatmika, 2021).

Bot Telegram, dikelola oleh sebuah Bot bernama Bot Father. Setelah membuat Bot, Bot Father akan mengirimkan Token API yang dapat kita gunakan pada website.



Gambar 1. Pembuatan Bot Telegram

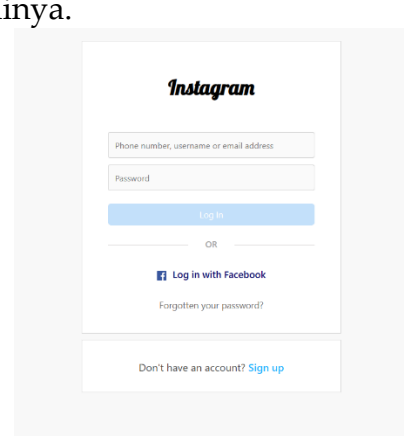
Token API dapat diterapkan pada *file javascript website*, sehingga *website* dapat mengirimkan pesan ke peretas.



Gambar 2. Insert API Telegram

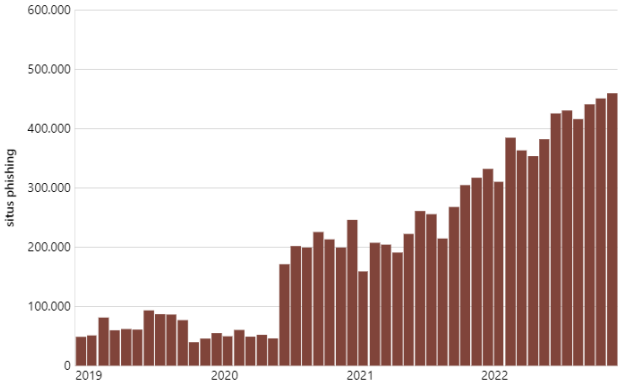
2. *User Interface* mirip

User Interface sangat berpengaruh terhadap keberhasilan *phising*. Tampilan yang mirip dengan *login page* Instagram yang asli, dapat membuat target tidak menyadari bahwa *login page* tersebut merupakan *login page* palsu. Situs web meminta Anda memasukkan informasi pribadi sensitif seperti kata sandi dan nama pengguna, yang pada akhirnya digunakan untuk pencurian identitas (Dm et al., 2022). Maka dari itu, kami mencoba merancang *User interface* yang mirip dengan aslinya.



Gambar 3. *User Interface* Instagram

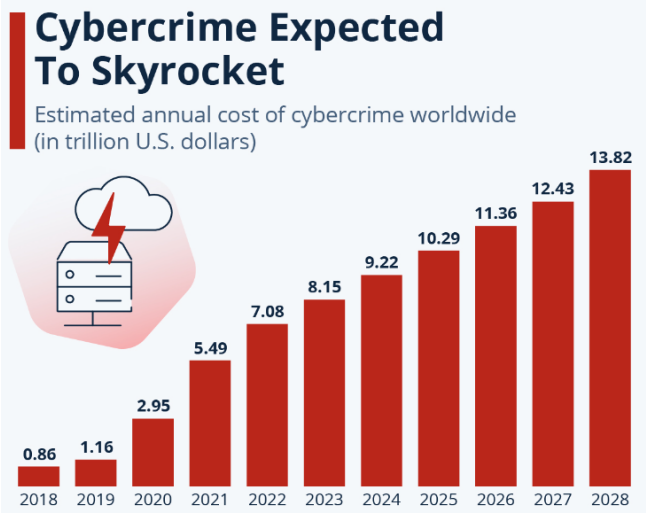
Hasil dan Pembahasan



Gambar 4. Grafik Tingkat *Phising*

Phishing adalah upaya memperoleh informasi pribadi seseorang dengan menggunakan teknik penipuan. Data yang biasanya di-*phishing* mencakup informasi pribadi (nama, umur, alamat), informasi akun (nama pengguna dan kata sandi), dan informasi keuangan (informasi kartu kredit, akun). Istilah resmi untuk *phishing* adalah *phishing*, dan asal usulnya adalah ``fishing'' yang berarti ``memancing.'' *Phishing* bertujuan untuk mengelabui orang agar mengungkapkan informasi pribadi tanpa sepengetahuan mereka. Informasi yang diberikan akan digunakan untuk tujuan kriminal (Wahyu Hidayat M et al., 2023).

Dari data statistik di atas, jumlah situs *phishing* dan penipuan semakin meningkat dari tahun ke tahun. Hal ini mungkin mempunyai implikasi lebih lanjut dan mengakibatkan kerugian baik bagi pengguna Internet maupun masyarakat umum atau institusi tertentu. Keamanan data menjadi hal yang sangat penting dikarenakan satu data dapat mengikat atau terhubung ke data yang lain. Seperti email yang terhubung pada media sosial atau nomor *handphone*.



Gambar 5. Grafik Kejahatan Siber

Pada tahun 2022, terjadi pembobolan di BRI di Sumatera Barat. Kejadian ini terungkap setelah korban menerima informasi melalui WhatsApp mengenai perubahan biaya transfer

dan mengklik tautan yang diberikan oleh pelaku. Korban kemudian mengisi formulir yang disediakan oleh pelaku, memberikan *username* dan *password*-nya. Akibatnya, korban mengalami kerugian sebesar 1,1 miliar rupiah. Laporan kejadian ini dibuat pada 31 Mei 2022 dan saat ini kasusnya sedang ditangani Reserse Kriminal Khusus Polda Sumbar. (Ginting et al., 2023).

Menilik kasus di atas dan data statistik dapat dipastikan jika *phising* ini dapat menimbulkan kerugian material yang tidak sedikit. Jika hal ini terus berlanjut maka akan timbul permasalahan lebih lanjut di banyak bidang. Agar dampak-dampak tersebut berkelanjutan, maka dampak-dampak tersebut perlu segera diatasi, atau setidaknya dicegah, dan kita perlu memperkuat kolaborasi dengan masyarakat luas agar lebih waspada.

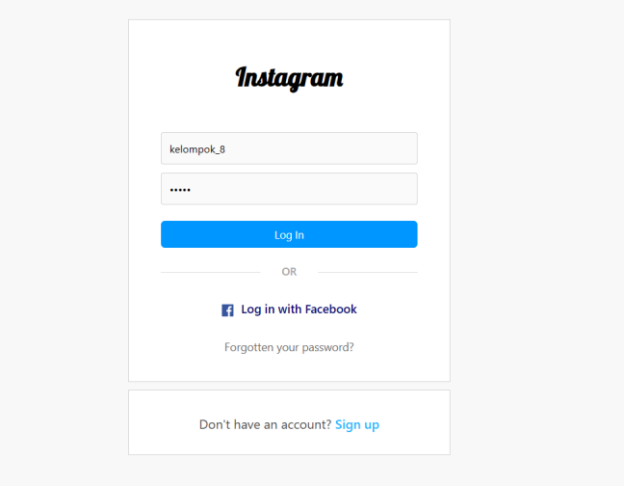
.

1. Simulasi *Phising* Menggunakan *Website* Penambah *Follower*

Dalam penerapan skema *phising*, kami membuat *website* yang saat ini sangat dicari-cari oleh kebanyakan orang, yaitu penambah *followers* instagram. Berikut merupakan hasil *website* yang telah kami buat.

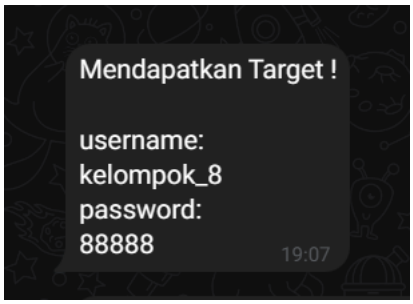
Gambar 6. Tampilan Awal Web

Tampilan awal *website* terdapat 1 buah tombol login yang akan mengarahkan target ke *login page* instagram palsu.

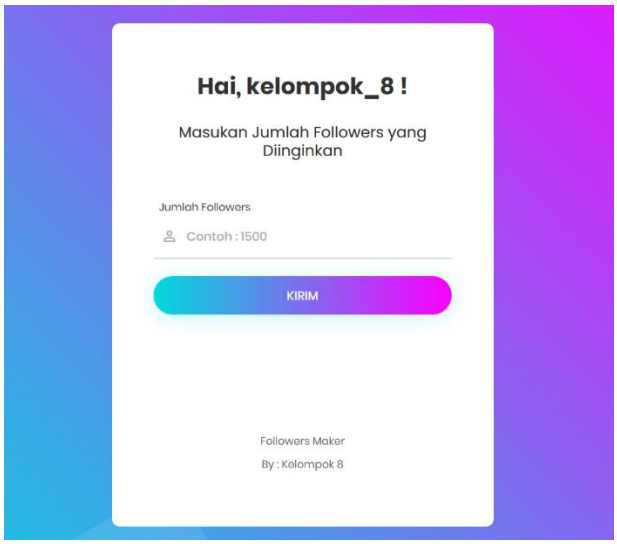


Gambar 7. Tampilan Halaman Login

Tampilan *login page* dibuat semirip mungkin dengan *login page* asli agar membuat target tidak menyadarinya.

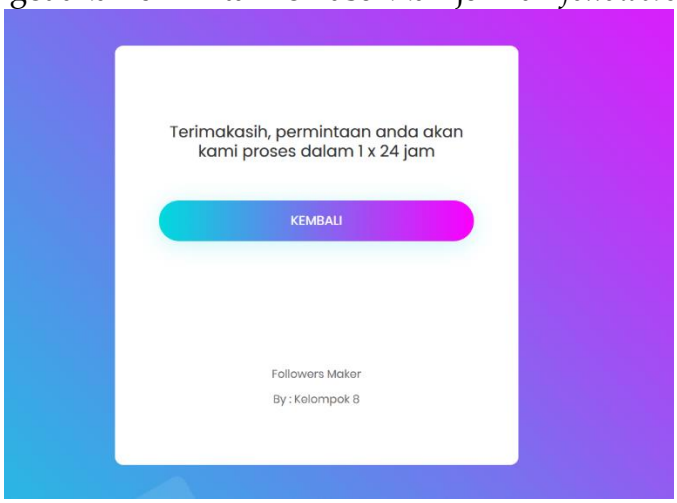


Gambar 8. Tampilan BOT Telegram



Gambar 9. Halaman Jumlah *Followers*

Ketika target menekan tombol *Login*, maka input kredensial dari target akan dikirimkan oleh Bot Telegram. Lalu *website* akan berpindah halaman seolah-olah target berhasil *login*. Lalu target akan diminta memasukkan jumlah *followers* yang diinginkan.



Gambar 10. Tampilan Akhir Web

Terakhir, agar target tidak curiga, akan muncul tampilan bahwa permintaan diproses. Sehingga, target akan mengira bahwa permintaan penambahan *follower* berhasil.

2. Pencegahan *Phising*

Melindungi diri dari serangan *phishing* merupakan langkah penting dalam mencegah kejahatan *cyber*. Tindakan pencegahan yang dapat dilakukan antara lain meningkatkan kesadaran dan mengedukasi pengguna tentang ancaman *phishing*, menggunakan perangkat lunak anti-*phishing*, mendeteksi situs web palsu, dan mendorong pengguna untuk tidak membagikan informasi sensitif kepada orang asing. Selain itu, organisasi juga perlu memastikan bahwa sistem keamanan mereka selalu diperbarui dan dipantau secara berkala untuk mendeteksi aktivitas mencurigakan yang berpotensi menjadi serangan *phishing* (Sinha & Kumar, 2018).

Serangan *phishing* merupakan salah satu jenis kejahatan dunia maya yang meningkat dalam beberapa tahun terakhir. Laporan mengatakan *phishing* menyebabkan kerugian ekonomi yang signifikan bagi individu dan organisasi di seluruh dunia. Oleh karena itu, upaya pencegahan harus dilakukan secara komprehensif, melibatkan kolaborasi multidimensi antara penegak hukum, industri teknologi informasi, organisasi keamanan informasi, perusahaan internet, dan institusi keuangan. Dengan bekerja sama, berbagi informasi, dan mengimplementasikan langkah-langkah keamanan terbaik, risiko terjadinya serangan *phishing* dapat diminimalisir dan dampak negatifnya dapat dikurangi (Das & Nayak, 2013).

Untuk mencegah serangan *phishing* yang memanfaatkan *malicious website*, pendekatan *machine learning* dapat digunakan untuk mengklasifikasi dan mendeteksi situs web tersebut. Sebuah studi yang menggunakan algoritma *K-Nearest Neighbor* (K-NN) untuk memprediksi situs web berbahaya berdasarkan lapisan aplikasi dan karakteristik jaringan terbukti efektif. Dengan melakukan seleksi fitur untuk memilih atribut yang paling berpengaruh, algoritma K-NN menghasilkan akurasi 93,61%, *recall* 85,05%, presisi 85,25%, dan RMSE 0,251 dalam mendeteksi dan mengklasifikasikan *malicious website* menggunakan 10-fold *cross validation*. Performa ini lebih baik dibandingkan dengan algoritme lain seperti pohon keputusan, regresi logistik, dan hutan acak. Penerapan teknik yang menggunakan pembelajaran mesin untuk mengklasifikasikan situs web berbahaya dapat diintegrasikan ke dalam sistem keamanan untuk membantu mendeteksi dan mencegah upaya *phishing* menggunakan situs web berbahaya (Sandag et al., 2018).

Selain menggunakan pendekatan teknologi, upaya preventif juga harus difokuskan pada peningkatan kesadaran dan edukasi bagi pengguna. Salah satu risiko utama terjadinya pencurian data pribadi yang berujung pada *phishing* adalah kurangnya pemahaman masyarakat tentang pentingnya melindungi informasi sensitif. Berdasarkan asas legalitas, pencurian data melanggar Undang-Undang Transaksi Informasi Elektronik (UU ITE). Oleh karena itu, data pribadi seseorang harus dilindungi sesuai dengan ketentuan yang berlaku, seperti peraturan Menteri Komunikasi dan Informatika dan peraturan Bank Indonesia.

Untuk mengatasi masalah tersebut, diperlukan tindakan preventif dan represif sesuai dengan teori perlindungan hukum dari Philipus M. Hadjon. Kampanye kesadaran mengenai keamanan data pribadi dan bahaya *phishing* harus digalakkan agar masyarakat lebih waspada dan mengambil tindakan pencegahan yang tepat (Bodhi & Tan, 2022).

Upaya preventif lainnya adalah dengan meningkatkan literasi keamanan siber di lingkungan kampus. Sebuah studi oleh Kusumaningrum dkk (2022), menggunakan MCDA untuk mengukur tingkat kesadaran keamanan siber siswa yang belajar di rumah. Hasilnya, tingkat kesadaran mahasiswa berada di level sedang (79,5%). Pengetahuan mahasiswa sudah baik (84%), namun sikap (78,3%) dan perilaku (73,1%) keamanan siber masih perlu ditingkatkan. Perguruan tinggi perlu memfasilitasi edukasi keamanan siber agar mahasiswa memiliki keterampilan melindungi diri dari ancaman seperti *phishing* selama pendidikan daring (Kusumaningrum et al., 2022).

Selain meningkatkan literasi keamanan pada kalangan mahasiswa, perguruan tinggi juga perlu melakukan *vulnerability assessment* secara berkala pada sistem dan aplikasi web untuk pembelajaran daring. Penelitian Orisa dan Ardita (2021) menunjukkan Nmap dapat digunakan untuk *vulnerability assessment* aplikasi web. Menggunakan *Nmap Scripting Engine* (NSE), kerentanan seperti open proxy HTTP, *cross-site scripting*, SQL injection dapat dideteksi. Temuan ini memungkinkan pengembang menutup celah keamanan sebelum dimanfaatkan pihak tidak bertanggung jawab. *Vulnerability assessment* penting untuk memastikan keamanan aset TI institusi dan keberlangsungan pendidikan daring yang aman dari kejahatan siber (Mira Orisa & Ardita, 2021).

Perkembangan teknologi informasi memberi banyak manfaat bagi industri dan perbankan, namun juga membuka celah bagi kejahatan *cyber* seperti *phishing*. Pada kuartal II 2014, layanan pembayaran menjadi sektor paling banyak diserang (39,8%), diikuti layanan keuangan. Perbankan pun rentan terhadap *phishing* melalui situs web palsu yang menipu dan mencuri identitas nasabah pengguna *online banking* (Muftiadi Amin, 2022).

Simpulan

Melalui penelitian ini, dapat disimpulkan bahwa, edukasi mengenai kejahatan *cyber* khususnya *phising* perlu ditingkatkan. Melalui data yang dipaparkan pada pembahasan, kejahatan *cyber* terus meningkat setiap tahunnya. Bahkan untuk melancarkan serangan siber ini tidak selalu menggunakan cara yang rumit. Tetapi dapat juga melalui cara yang mudah seperti *phising*.

Dari contoh penerapan yang diberikan, bahwa membuat *phising* sangatlah mudah, bahkan dapat menggunakan BOT Telegram. Pengguna yang tertipu oleh serangan ini dapat mengalami pencurian identitas, akses tidak sah ke akun mereka, dan penyalahgunaan data pribadi. Maka dari itu, peningkatan edukasi kepada masyarakat mengenai membedakan *website* palsu dengan yang asli sangat penting untuk dilakukan.

Daftar Pustaka

Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cybercrime). *UNES Law Review*, *4*(3), 297–308. https://doi.org/10.31933/unesrev.v4i3.236

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234.

https://doi.org/10.54706/senastindo.v3.2021.141
Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447
Das, S., & Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142–153.
Dm, M. Y., Addermi, & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling*, *4*(5), 8018–8023.
Ginting, E., Sinaga, M. P., Nurdin, M. R., & Putra, M. D. (2023). Analisis Ancaman Phising Terhadap Layanan Online Perbankan (Studi Kasus Pada Bank BRI). *UNES Journal of Scientech Research*, *8*(1), 41–47. https://ojs.ekasakti.org/i
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
Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. https://doi.org/10.17933/mti.v8i2.108
Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal TIMES*, *V*(2), 35–42.
Kharisma Putra, I. K. O., Darmawan, I. M. A., Juliana, I. P. G., & Indriyani. (2023). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising. *Cyber Security Dan Forensik Digital*, *5*(2), 77–82. https://doi.org/10.14421/csecurity.2022.5.2.3797
Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, *20*(1), 69. https://doi.org/10.30646/sinus.v20i1.586
Mira Orisa, & Ardita, M. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web. *Jurnal Mnemonic*, *4*(1), 16–19. https://doi.org/10.36040/mnemonic.v4i1.3213
Muftiadi Amin, A. M. P. T. E. M. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking. *Jurnal.Arkainstitute*, *1*(2), 1–6.
Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*(01), 14–20.
Sandag, G. A., Leopold, J., & Ong, V. F. (2018). Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics. *CogITo Smart Journal*, *4*(1), 37–45. https://doi.org/10.31154/cogito.v4i1.100.37-45
Sinha, R., & Kumar, H. (2018). A Study on Preventive Measures of Cyber Crime. *International Journal of Research in Social Sciences*, *8*(11), 265–272. https://doi.org/10.13140/RG.2.2.14212.04480
Sudiatmika, I. P. G. A. (2021). E-Learning Berbasis Telegram Bot. *KERNEL: Jurnal Riset*

Inovasi Bidang Informatika Dan Pendidikan Informatika, *1*(2), 49–60. https://doi.org/10.31284/j.kernel.2020.v1i2.1469

Wahyu Hidayat M, Hartini Ramli, Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek : Jurnal Pengabdian Masyarakat*, *1*(1), 28–33. https://doi.org/10.61255/vokatekjpm.v1i1.29

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *JOEICT(Jurnal of Education and Information Communication Technology)*, *1*(1), 1–5. https://www.jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

Yudha, F., Muhammad, A., & Muryadi, P. (2018). CyberSecurity dan Forensik Digital PERANCANGAN APLIKASI PENGUJIAN CELAH KEAMANAN PADA APLIKASI BERBASIS WEB. *CyberSecurity Dan Forensik Digital*, *1*(1), 1–6.