CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, hlm. 77-82

TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK *PHISING*

I Kadek Odie Kharisma Putra[1], I Made Adi Darmawan[2], I Putu Gede Juliana[3], Indriyani[4]

[1,2,3,4] ITB STIKOM Bali

Email: [1]odiekharisma@gmail.com, [2]adidarmawan2705@gmail.com, [3]gedejuliana234@gmail.com, [4]indry.joice@gmail.com

Abstrak

Perkembangan teknologi informasi, khususnya komunikasi internet, telah membawa perubahan besar secara nasional, ekonomi dan budaya. Perkembangan teknologi informasi ini pada gilirannya mengubah tatanan dan perilaku sosial, khususnya dalam satu dekade terakhir penggunaan teknologi informasi berkembang pesat. Pada satu sisi informasi dapat memberikan manfaat, mempermudah dan mempercepat akses informasi yang kita butuhkan dalam segala hal dan dapat mengubah model ekonomi dan model bisnis. Namun, banyak dampak negatif yang muncul dan tidak dapat dihindari karena internet sudah menjadi bagian dari aktivitas sehari-hari semua orang dalam mengakses berbagai macam informasi dan juga membantu atau meringankan pekerjaan setiap orang.

Kata Kunci: *Cyber Crime*, Dunia Digital

CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING

Abstract

The development of information technology, especially internet communication, has brought major changes nationally, economically and culturally. The development of information technology has in turn changed social order and behavior, especially in the last decade the use of information technology has grown rapidly. On the one hand, information can provide benefits, simplify and speed up access to the information we need in every way, and can change economic models and business models. However, many negative impacts arise and cannot be avoided because the internet has become part of everyone's daily activities in accessing various kinds of information and also helping or lightening everyone's work.

Keywords*: Cyber Crime, Digital World*

1. PENDAHULUAN

Teknologi informasi mampu mengubah realitas ekonomi, budaya, politik, dan hukum. Seiring berkembangnya teknologi informasi mampu memberikan dampak positif bagi banyak orang namun hal ini juga menyebabkan munculnya kejahatan-kejahatan baru yang disebut dengan kejahatan dunia maya baru melalui jaringan internet. Dimana terdapat beberapa orang yang memanfaatkan celah keamanan pada teknologi informasi pada jaringan internet sebagai sarana untuk melakukan kejahatan yang selanjutnya dikenal dengan *cybercrime*.

Cybercrime merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan *carding*, *hacking*, penipuan, terorisme, dan penyebaran informasi yang mengganggu menjadi bagian dari aktivitas pelaku *cybercrime* (Gulo, Ardi Saputra; Sahuri, Lasmadi; Khabib, Nawawi;, 2021).

Kejahatan dunia maya adalah kasus pelanggaran yang melibatkan komputer atau alat komunikasi sebagai target dan instrumen komisi atau terkait dengan prevalensi komputer.

Kejahatan dunia maya atau *cybercrime* menelan biaya hampir sebesar 6 triliun *dollar* per tahun pada tahun 2021 sesuai dengan laporan usaha keamanan *cyber* pada tahun 2020. Untuk kegiatan ilegal, penjahat dunia maya menggunakan perangkat komputasi jaringan apapun sebagai sarana utama untuk berkomunikasi dengan perangkat korban, sehingga penyerang mendapatkan keuntungan dari segi keuangan, publisitas dan orang lain dengan mengeksploitasi kerentanan atas sistem.

Kejahatan dunia maya terus meningkat setiap hatinya, mengevaluasi serangan kejahatan dunia maya dan memberikan tindakan perlindungan dengan metode manual menggunakan yang ada pendekatan bisnis dan juga investigasi seringkat gagal dalam mengendalikan serangan *cybercrime*. Bentuk umum dari kejahatan dunia maya adalah *carding*, *hacking*, *phising*, terorisme, Penyebaran informasi yang mengganggu merupakan bagian dari aktivitas kriminal di dunia maya. Gugatan di dunia maya pasti ada hubungannya dengan mengapa seseorang melakukan kejahatan dunia maya. Karena perlu Anda ketahui bahwa ketika kejahatan dunia maya dilakukan, pihak lain tentu akan dirugikan. *Cybercrime* tidak hanya dikenal sebagai peretasan atau *hacking*, tetapi juga dikenal sebagai *cracking* atau perengkahan, dan perlu dicatat bahwa ada persamaan dan perbedaan antara peretasan dan

perengkahan. Salah satu kejahatan yang dilakukan *cracker* ini adalah *phishing*. Karena kejahatan ini bertujuan untuk mengeksploitasi diri sendiri. *Phising* adalah suatu bentuk aktivitas dimana seseorang diancam atau ditangkap dengan konsep memancing orang tersebut (Marliani, Miftahudin Siagian;, 2017).

Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tentu saja, sebagian besar kejahatan dunia maya biasanya dimulai dengan *phising*, sehingga pengguna internet harus selalu waspada. *Phising* juga biasanya menyasar pengguna *online banking*, karena penggunaan data pengguna dan kata sandi tidak menutup kemungkinan dialihkan ke pengguna *online* lainnya. Saat pengguna memasukkan kredensial pengguna dan kata sandi mereka ke dalam formulir *login*, yang merupakan formulir *login* palsu, penjahat dunia maya dapat mengetahuinya dalam bentuk *phising*. *Phising* biasanya dilakukan melalui media sosial yang terhubung dengan *internet*, seperti melalui *email* atau SMS dan *website*. Pengetahuan pengguna yang minim tentang alat teknologi informasi yang digunakan adalah yang mendorong *phising*. *Phishing* dapat terjadi di berbagai *platform*, termasuk media sosial, situs *web*, dan juga aplikasi. Saat ini, banyak orang yang menggunakan aplikasi WhatsApp sebagai aplikasi untuk bertukar pesan, dan Instagram sebagai aplikasi yang memungkinkan pengguna untuk mengambil foto dan video serta membagikannya untuk diperlihatkan kepada banyak orang. Hal ini pun dimanfaatkan oleh orang tidak bertanggung jawab dan menggunakannya untuk kejahatan. Pada WhatsApp, penjahat mencoba mengirim pesan ke nomor tertentu. Pesan ini mungkin berisi informasi bahwa nomor ini telah dipilih sebagai pemenang lotre, dan ketika pengguna menekan *link* tersebut, mereka diminta untuk mengonfirmasi melalui *link* tersebut. Pengguna akan dibawa ke situs *web* berbahaya yang telah dimodifikasi oleh pelaku.

Mirip dengan aplikasi Instagram, tindakan kriminal ini dapat dilakukan melalui pesan langsung dan komentar pada postingan. Misalnya pada *Direct Messages*, seorang pengguna menerima pesan dari pengguna lain yang berisi informasi yang menggiurkan bahwa pengguna tersebut berpeluang memenangkan hadiah, dan akan dicantumkan sebuah *link* dimana pengguna tersebut dikirim ke situs *web* berbahaya yang dijalankan oleh orang yang tidak bertanggung jawab. Cara lainnya adalah dengan komentar pada postingan dimana salah satu pengguna akan memposting foto atau video yang berisi informasi tentang insiden yang menarik bagi pengguna lain. Jadi, pengguna yang lain akan dibuat penasaran mengenai informasi lengkap dari postingan tersebut sehingga pengguna yang lain akan mengirimkan sebuah *link* dimana pengguna tersebut meyakinkan bahwa kita akan mendapatkan informasi lengkap dari postingan yang telah dibuat. Sehingga, pengguna yang lainnya akan mencoba mengirimkan sebuah *link* dan meyakinkan pengguna lainnya untuk menekan *link* tersebut dikarenakan pada *link* tersebut terdapat informasi lengkap mengenai apa yang dijelaskan pada postingan tersebut. Padahal *link* tersebut bisa saja terdapat virus atau pengguna akan dibawa ke situs berbahaya yang dapat mengancam keamanan pengguna yang mengakses.

Kejahatan bisa terjadi di mana saja, bahkan di dunia maya. Jadi pengguna harus selalu waspada dalam menggunakan internet karena masih banyak orang yang belum memiliki pengetahuan yang cukup untuk mengakses *internet* dan oknum-oknum yang tidak bertanggung jawab mencoba memanfaatkan orang-orang tersebut. Ketidaktahuan pengguna mengenai hal-hal yang ada di *internet* yang membuat pengguna terjerumus dalam korban tindakan kejahatan dunia maya. Oleh karena itu, saat bertukar pesan dengan orang asing atau mendapatkan informasi yang dikirim oleh orang lain, pengguna harus selalu waspada dan memastikan bahwa pengguna dapat memverifikasi keakuratan informasi yang diberikan. Pengguna harus selalu memastikan bahwa informasi yang dikirimkan oleh orang lain benar atau tidak melalui situs-situs resmi dan juga jangan mudah percaya apabila menerima informasi bahwa pengguna memenangkan suatu hadiah dan orang tersebut mengirimkan sebuah *link* karena bisa saja *link* tersebut terdapat hal-hal yang berbahaya yang dapat mengancam keselamatan perangkat dan juga pengguna.

2. TINJAUAN PUSTAKA

Kajian pustaka yang digunakan dalam artikel ini merupakan teori yang mendasari artikel. Selain itu, kajian pustaka juga dilakukan melalui jurnal penelitian nasional dan internasional. Saat menulis artikel ini, penulis terlebih dahulu mencoba menghubungkan beberapa jurnal untuk menghubungkan dengan artikel ini. Jurnal yang dirujuk oleh penulis yaitu:

Jurnal Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, Fakultas Hukum, Universitas Jambi dengan judul: *Cyber Crime* dalam Bentuk *Phising* berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. Jurnal ini meliput kejahatan dunia maya seperti *phising* berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. Adapun hasil dari jurnal ini ialah pengaturan hukum kejahatan dunia maya berupa *phising* berdasarkan Undang-Undang Informasi dan Transaksi Elektronik tunduk pada Pasal 35 jo Pasal 51 Ayat (1) dan Pasal 28 Ayat (1) jo Pasal 45A Ayat (1). , kebijakan hukum terhadap *cybercrime* berupa *phising* berdasarkan Undang-Undang Informasi dan Transaksi Elektronik mengubah undang-undang tentang ITE dengan merumuskan konsep *phising* dan mengubah isi Pasal 35.

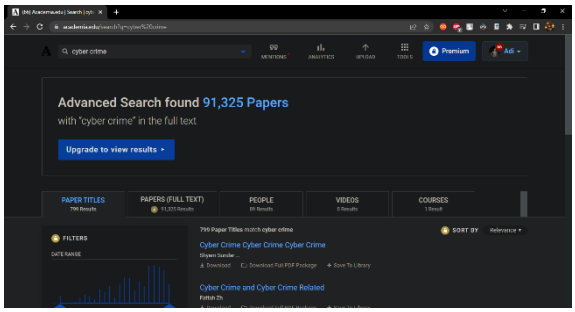
3. METODE PENELITIAN

Dengan adanya permasalahan tersebut, maka tulisan ini akan mengkaji tentang perkembangan

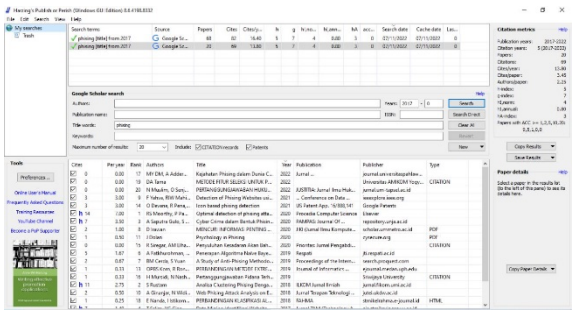
tindakan *cybercrime* dalam bentuk *phising* menggunakan metode kajian sistematis (*systematic review*). Pada pembahasan ini dilakukan peninjauan secara sistematis dengan memilih terlebih dahulu dan menentukan daftar jurnal yang terkait dengan *cyber crime*. Dimulai dari mencari jurnal yang membahas tentang dunia digital, perkembangan teknologi, dan berlanjut ke kejahatan dunia maya atau *cybercrime*, pada akhirnya penulis mendapatkan jurnal yang membahas mengenai tindakan kejahatan dunia digital dalam bentuk *phising*.

Berikut merupakan beberapa tangkapan layar pada saat pencarian beberapa jurnal untuk kebutuhan penulisan karya ilmiah ini :

Gambar 1 Pencarian Jurnal di Google Schoolar



Gambar 2 Pencarian Jurnal di Academia



Gambar 3 Pencarian Jurnal melalui Publish or Perish

4. HASIL DAN PEMBAHASAN

Kejahatan siber dengan metode *phising* seringkali ditemukan pada *platform* media sosial. Media sosial menjadi sasaran utama *hacker* untuk menjalankan aksinya karena media sosial memiliki banyak pengguna dan sangat bebas tanpa adanya suatu filter. Kurangnya edukasi terhadap penggunaan media sosial, memudahkan *hacker* untuk melakukan suatu penipuan-penipuan. Media sosial yang paling banyak terjadinya *phising* yaitu WhatsApp dan Facebook. Media sosial Facebook seringkali digunakan untuk mencuri data dari pengguna. *Hacker* memanfaatkan tampilan Facebook untuk dibuatkan duplikat tampilan yang palsu.

Ketika pengguna tidak sengaja masuk ke halaman palsu dan melakukan registrasi atapun *login*, maka *hacker* akan langsung mendapatkan data privasi dari pengguna.

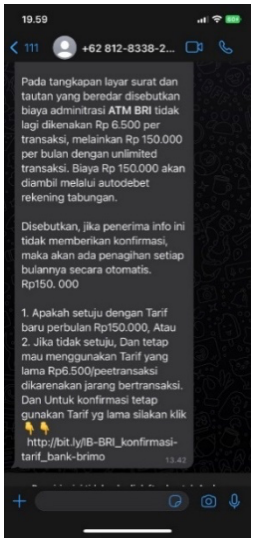
Selain dari media sosial, *website* juga merupakan salah satu target para *hacker* untuk melakukan *phising*. Dengan memanfaatkan iklan dan *icon* palsu pada *website* yang dapat di klik oleh pengguna, maka pengguna akan diarahkan pada suatu *link* yang sudah dikonfigurasi oleh *hacker* untuk mencuri data. Sangat banyak kasus seperti ini khususnya pada kalangan pelajar. Penipuan yang pernah terjadi adalah penerimaan kuota gratis yang diselenggarakan oleh Kemendikbud. Hal ini dimanfaatkan *hacker* untuk membuat *link-link* palsu yang berisi informasi penerimaan kuota gratis. Saat ini, kejahatan siber dengan metode *phising* telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dengan adanya undang-undang ini, ketika ada orang yang teridentifikasi melakukan *phising*, maka orang tersebut akan dikenakan suatu hukuman sesuai dengan apa yang tertera didalam undang-undang. Korban dapat melaporkan kejahatan ini pada pihak yang berwenang untuk dilakukannya investigasi.

Berdasarkan hasil yang telah dianalisis, bahwa tindak kejahatan *phising* bisa dilakukan dari berbagai contoh penyerangan seperti melalui berbagai jenis media sosial dan *website*, jika pengguna tidak teliti dalam menggunakan media sosial dan mengunjungi *website* yang telah dimodifikasi oleh pelaku maka sangatlah mudah untuk pelaku mengambil data privasi pengguna. Dari beberapa kasus yang dipaparkan, tindakan *phising* sering terjadi pada *platform* media sosial seperti WhatsApp dan Facebook dimana banyak pelaku yang melancarkan tindakannya dengan mengatasnamakan instansi resmi dan seolah-olah bertindak dari pegawai resmi instansi tersebut dimana jika secara tidak sadar bahwa pengguna yang ditargetkan menuruti keinginan pelaku untuk menyukseskan aksinya.

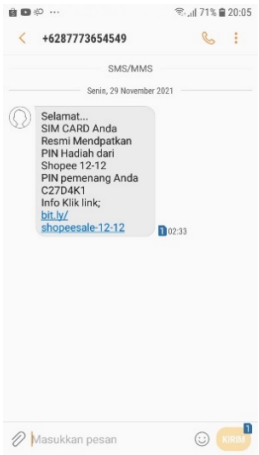
Tabel 1 Catatan Layar Bukti Penipuan

No.	Aplikasi	Tanggal/Waktu	Bentuk
1.	WhatsApp	27-09-2022/13:42:00 Wita	*Chat* dan *Link*
2.	SMS	29-11-2021/02:33:00 Wita	*Chat* dan *Link*
3.	WhatsApp	07-11-2022/17:10:00 Wita	*Chat* dan *Gambar*

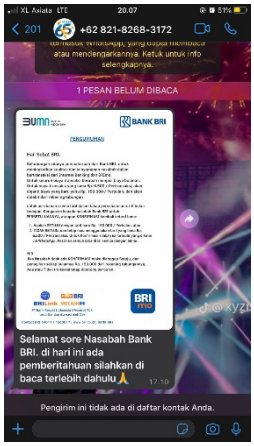
Hasil penelitian yang dilakukan didasarkan pada pencarian data tentang penipuan asli yang terjadi di *platform* media sosial. Penipuan yang terjadi terdiri dari penerimaan pesan dari *hacker* dengan kedok menawarkan keuntungan kepada penerima pesan. Berikut adalah bukti nyata penerimaan pesan palsu dari *hacker*.



Gambar 4 Bukti Kasus Penipuan Pada WhatsApp (Chat dan Link)



Gambar 5 Bukti Kasus Penipuan Pada SMS (Chat dan Link)



Gambar 6 Bukti Kasus Penipuan Pada WhatsApp (Chat dan Gambar)

Pelaku tindakan *phising* melancarkan aksinya dengan menggunakan *link* ataupun *icon* bergambar untuk mempermudah aksinya agar pengguna percaya bahwa hal yang diberikan oleh pelaku adalah resmi. Dari hal tersebut pelaku sudah mendapatkan kepercayaan pengguna sehingga pelaku dapat melanjutkan aksinya untuk mendapatkan data privasi dan memenuhi keinginan yang dapat merugikan pengguna. Dengan pemaparan diatas penulis menyarankan agar pengguna selalu berhati-hati dalam dunia digital dan tidak berkunjung sembarangan terutama menggunakan media sosial dan *website*, diharapkan pengguna selalu memastikan bahwa jika ada konteks atau hal yang palsu atau melenceng dapat dicek kembali keresmiannya melalui media-media resmi dari konteks tersebut dan dapat melaporkan ke pihak berwajib sehingga dapat dikenakan pasal yang terkait.

5. KESIMPULAN DAN SARAN

Kejahatan dunia maya adalah kasus pelanggaran yang melibatkan komputer atau alat komunikasi sebagai target dan instrumen komisi atau terkait dengan prevalensi komputer. Bentuk dari kejahatan ini sangat beragam sehingga *hacker* dapat memilih metode yang mereka ingin gunakan untuk melancarkan aksi kejahatan di dunia maya.

Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tindakan *phising* sering terjadi pada media sosial khususnya pada aplikasi WhatsApp dan Facebook. Salah satu kasus kejahatan *phising* yang pernah terjadi yaitu kasus penerimaan kuota gratis yang diselenggarakan oleh Kemendikbud.

Tindakan kejahatan dunia maya seluruhnya diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dengan adanya undang-undang ini, ketika ada orang yang teridentifikasi melakukan *phising* ataupun tindakan kejahatan dunia maya lainnya, maka orang tersebut akan dikenakan suatu hukuman sesuai dengan apa yang tertera didalam undang-undang.

Tindakan kejahatan dunia maya dapat menyasar berbagai kalangan, mulai dari kalangan masyarakat, organisasi, pemerintahan, dan lainnya. Maka dari itu, sebagai pengguna yang sering berselancar di dunia maya, sebaiknya selalu berhati-hati dan tidak mudah percaya dengan semua hal yang ada di dunia maya. Selain itu, pengguna juga harus mempelajari setiap hal baru yang terdapat di dunia maya guna untuk mencegah terkena dampak dari tindakan kejahatan.

DAFTAR PUSTAKA

CASCAVILLA, G., TAMBURRI, D. A., & VAN DEN HEUVEL, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers and Security, 105, 102258. https://doi.org/10.1016/j.cose.2021.102258.

AL-KHATER, W. A., AL-MAADEED, S., AHMED, A. A., SADIQ, A. S., & KHAN, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE Access, 8, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

CH, R., GADEKALLU, T. R., ABIDI, M. H., & AL-AHMARI, A. (2020). Computational system to classify Cyber Crime offenses using machine learning. Sustainability (Switzerland), 12(10). https://doi.org/10.3390/SU12104087

FAHLEVI, M., SAPARUDIN, M., MAEMUNAH, S., IRMA, D., & EKHSAN, M. (2019). Cybercrime Business Digital in Indonesia. E3S Web of Conferences, 125(201 9), 1–5. https://doi.org/10.1051/e3sconf/201912521001

KOTO, I. (2021). IJRS: International Journal Reglement & Society Cyber Crime According to… Cyber Crime According to the ITE Law. August, 103–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs

PARANDE, S. (2021). and Engineering Trends. Engineering, 6(1), 2020–2022.

SADIQ, A., ANWAR, M., BUTT, R. A., MASUD, F., SHAHZAD, M. K., NASEEM, S., & YOUNAS, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5), 854–864. https://doi.org/10.1002/hbe2.301

RUSTAM, S. (2018). Analisa Clustering Phising Dengan K-Means Dalam Meningkatkan Keamanan Komputer. ILKOM Jurnal Ilmiah, 10(2), 175–181. https://doi.org/10.33096/ilkom.v10i2.309.175-181.

HAYATI, M., & FATA, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising. Djtechno Jurnal Teknologi Informasi, 2(1), 21–28. https://doi.org/10.46576/djtechno.v2i1.1252.

EFENDY, Z., PUTRA, I. E., & SAPUTRA, R. (2019). Asset Rental Information System and Web-Based Facilities At Andalas University. Jurnal Terapan Teknologi Informasi, 2(2), 135–146. https://doi.org/10.21460/jutei.2018.22.103

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

Informatika Universitas Buddhi Dharma Jl Imam Bonjol No, T., & Ilir Tangerang Banten, K. (2017). Data Mining Identifikasi Website Phising Menggunakan Algoritma C4.5 Tomy Salim 1) Yo Ceng Giap 2). Technology Acceptance Model, 8, 130–135.

MISHRA, A., & FANCY. (2021). Efficient Detection of Phising Hyperlinks using Machine Learning. International Journal on Cybernetics & Informatics, 10(2), 23–33. https://doi.org/10.5121/ijci.2021.100204.

MARLIANI, SIAGIAN, M. (2017). Jurnal Pendidikan dan Konseling. Al-Irsyad, 105(2), 79. https://core.ac.uk/download/pdf/322599509.pdf.

IRAWAN, D. (2020). Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising. JIKI (Jurnal Llmu Komputer & Lnformatika), 1(1), 43–46. https://doi.org/10.24127/jiki.v1i1.671.

MOORTHY, R. S., & PABITHA, P. (2020). Optimal Detection of Phising Attack using SCA based K-NN. Procedia Computer Science, 171(2019), 1716–1725. https://doi.org/10.1016/j.procs.2020.04.184.

RAMADHAN, A., ALHAFIDH, M. A., & FIRMANSYAH, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS. Kampret Journal, 1(1), 11–15. https://doi.org/10.35335/kampret.v1i1.9.

MUSLIM, N., SENJAYA, O., HUKUM, F., & KARAWANG, U. S. (2022). Pertanggungjawaban Hukum Platform Media Sosial Terhadap Korban Phising Melalui Mass Tagging. 9(2), 955–963.

ALMSEIDIN, M., ABU ZURAIQ, A. M., AL-KASASSBEH, M., & ALNIDAMI, N. (2019). Phishing detection based on machine learning and feature selection methods. International Journal of Interactive Mobile Technologies, 13(12), 71–183. https://doi.org/10.3991/ijim.v13i12.11411

CHARAN, A. N. S., CHEN, Y. H., & CHEN, J. L. (2022). Phishing Websites Detection using Machine Learning with URL Analysis. Proceedings - 2022 IEEE World Conference on Applied Intelligence and Computing, AIC 2022, 808–812. https://doi.org/10.1109/AIC55036.2022.9848895

ALABDAN, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches.

Future Internet, 12(10), 1–39. https://doi.org/10.3390/fi12100168

RACHMAWATI, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber.

Jurnal Ilmiah Saintikom, Universitas Sumatera Utara, Medan, 1978–6603, 209–216

Dolan, J. (2020). Psychology in Phishing Jonathan Dolan IASP 470 System Security Capstone March 17

Latifahi, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19. Islamic Banking and Finance Journal, 6(1), 73–85. https://doi.org/10.21070/perisai.v6i1.

Wahyudi, D., Niswar, M., (2022). Website Phising Detection Application Using Support Vector Machine (Svm). Journal of Information, 5(2). https://media.neliti.com/media/publications/432156-none-2b0098ce.pdf