Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 8, Nomor 1, Februari 2023, pp 117-125
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau

Koko Caniago[1], Tata Sutabri[2]
[1]Program Studi Magister Teknik Informatika, Universitas Bina Darma, Palembang, Indonesia
[2]Universitas Bina Darma, Palembang, Indonesia
Email: [1]kokocaniago2@gmail.com, [2] Tata.Sutabri@gmail.com

Abstract

The rapid advancement of today's technology is very helpful for someone in doing work, one of the technologies that is very developed today is the internet, with the internet, it is very easy for someone to communicate with other people, access data stored on the internet and make it very easy for someone to do their job. but behind the convenience when accessing the internet there are crimes that can attack internet users themselves, one of the crimes is phishing, where phishing is very detrimental to the victim. Phishing is a threat that uses social engineering techniques to trick users by impersonating an authorized entity. Phishing attacks various industrial sectors including the corporate industry, banking, education and others. Factors that cause phishing in online banking services are the lack of user knowledge, psychology, and privacy of social networking services. Therefore, prevention of phishing attacks can be done through computer network security. The research method used in this study is a qualitative method with descriptive techniques.

Keywords*: Phishing, Internet, Research methods*

Abstrak

Pesatnya kemajuan teknologi zaman sekarang sangat membantu sesorang dalam melakukan pekerjaan, salah teknologi yang sangat berkembang saat ini adalah internet, dengan adanya internet maka sesorang sangat mudah berkomunikasi dengan orang lain, mengakses data yang disimpan di internet dan sangat mempermudah akses sesorang untuk melakukan pekerjaannya, akan tetapi dibalik kemudahan saat mengakses internet terdapat tindak kejahatan yang bisa menyerang pengguna internet itu sendiri, salah satu tindak kejahatanya yaitu phising, dimana phising sangat merugikan korbanya. Phising adalah ancaman yang menggunakan teknik rekayasa sosial yang mengelabui pengguna dengan meniru identitas entitas yang berwenang. Phishing menyerang berbagai sektor industri termasuk industri perusahan, perbankan , pendidikan dan lain-lain. Faktor penyebab terjadinya phishing pada layanan publik adalah minimnya pengetahuan pengguna, psikologi, dan privasi layanan jejaring sosial. Oleh karena itu, pencegahan serangan phising dapat dilakukan melalui pengamanan jaringan komputer. Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif dengan teknik deskriptif.

Kata kunci: *Phishing, Internet, Metode penelitian*

I. PENDAHULUAN

Kemudahan mengkases internet seperti saat ini sangat membantu pekerjaan sesorang, sehingga sesorang sering mengakses data-data melalalui internet dengan kemudahan tersebut tidak membuat sesorang bisa aman dalam menggunakan internet karena banyak ancaman yang bisa terjadi yang bisa merugikan pengguna internet tersebut, salah satu ancaman yang bisa mengacam adalah phising yang menjadi salah satu kejahatan internet yang sangat meresakan pengguna internet. Phishing adalah aktivitas cyber crime yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data identitas dan kredensial akun . Skema rekayasa sosial dilakukan dengan menggunakan email palsu yang mengaku berasal dari institusi bisnis yang sah dan dirancang untuk mengarahkan korban ke situs web

palsu yang mengelabui, sehingga korban membocorkan data keuangan seperti : nama dan kata sandi. Skema subterfomen teknis menanam crimeware ke PC untuk mencuri kerahasiaan secara langsung, sering menggunakansistem untuk mengelabui nama pengguna dan kata sandi akun online dan merusak infrastruktur navigasi lokal untuk menyesatkan konsumen ke situs web palsu (atau situs web asli melalui proxy yang dikendalikan phiser yangdigunakan untuk memantau dan intercept pada konsumen).Karna maraknya kejahatan phishing yang terjadi di internet maka peneliti ingin mengakat judul tentang tindak kejatan phising terhadap sektor layanan publik, dimana peniliti melakukan penelitian di Universitas Bina Insan. Peneliti akan melakukan wawancara kepada beberapa staff pelayanan Universitas Bina Insan, apakah pernah terjadi tindak kejatahan phishing di sektor pelayanan Universitas Bina Insan.

2. METODOLOGI PENELITIAN

2.1. Cyber Crime

Menurut Organization of European Community Development(OECD) cyber crimeadalah semua bentuk akses ilegal terhadap suatu transmisi data. Artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan.Secara umum,pengertiancyber crime sendiri memang biasa diartikan sebagai tindak kejahatan di ranah dunia maya yang memanfaatkan teknologi komputer dan jaringan internet sebagai sasaran.Tindakan cyber crimeini muncul seiring dengan kian gencarnya teknologi digital, komunikasi dan informasi yang semakinberkembang [1].

2.1. Hacking

Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi [2].

2.2. Phising

Phising yaitu suatu tindakan untuk memperoleh informasi pribadi seperti User ID, PIN,nomor rekening bank, nomor kartu kredit Anda secara tidak sah. Informasi ini kemudian akandimanfaatkan oleh pihak penipu untuk mengakses rekening, melakukan suatu penipuan kartu kredit atau memandu nasabah agar melakukan perbuatan transfer ke rekening tertentu dengan iming-iming sebuah hadiah [3].

2.3. Penelitian Terdahulu

Dalam pembuatan jurnal Tindak Kejahatan Phising ini penulis menggunakan beberapa referensi jurnal di antaranya :

a) Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking [4].
b) Analisis Serangan Web Phising pada layanan e-commerce dengan metode network forensic process [5].
c) Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling.[6]

d) Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan.[7]
e) Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising.[8]

2.4. Metode Penelitian

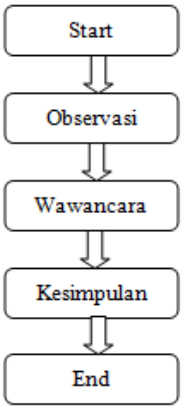
Metode penelitian adalah cara yang digunakan untuk memecahkan masalah yang akan diteliti selama penelitian berlangsung. Saat menulis artikel ini, peneliti menggunakan metode penelitian [9].

Penelitian kualitatif adalah penelitian yang menekankan pada kualitas atau hal terpenting dalam sifat suatu barang atau objek. Yang terpenting dalam barang atau jasa berupa peristiwa/fenomena/gejala sosial adalah makna di balik peristiwa tersebut, yang dapat dijadikan pelajaran berharga untuk mengembangkan konsep teoritis [10].

Oleh karena itu, jenis penelitian kualitatif yang digunakan adalah penelitian deskriptif dengan menggunakan metode penelitian kepustakaan. Kritik sastra merupakan metode penelitian yang dilakukan untuk mengkaji dan mempertimbangkan secara kritis masalah yang diteliti. Peneliti akan menggunakan sumber data sekunder yang diperoleh dari dokumen, arsip, buku, makalah, makalah, dan hasil penelitian lainnya. Dalam metode analisis data, Milles dan Huberman (1984) menyatakan bahwa ada beberapa langkah yang perlu dilakukan peneliti dalam melakukan analisis data, yaitu reduksi data, display data, dan inferensi atau validasi. Oleh karena itu, dalam artikel tentang Contoh praktis keamanan. Jaringan komputer: analisis ancaman phishing di sektor layanan Universitas Bina Insan Lubuklinggau.

2.5. Kerangka Berpikir

Kerangka berpikir dalam penelitian ini bisa dilihat pada gambar di bawah ini :



Gambar 1. Kerangka Penelitian

2.6. Teknik Pengumpulan Data

Universitas Bina Insan Lubuklinggau yang beralamat Jl. HM Soeharto No.Kel, Lubuk Kupang, Kec. Lubuk Linggau Sel. I, Kota Lubuklinggau, Sumatera Selatan 31626. Pengambilan data secara langsung harus dilakukan di sana. Berikut ini adalah teknik pengumpulan datanya:

a) Metode Observasi
Peneliti Melakukan pengamatan secara langsung di Universitas Bina Insan Lubuklinggau peneliti menemui kepala Perpustakaan dan Kepala ICT Universitas Bina Insan.
b) Metode Wawancara
Peneliti mewancarai secara langsung dengan kepala perpustakaan Universitas Bina Insan Lubuklinggau dan Kepala ICT Universitas Bina Insan Lubuklinggau [12].
c) Dokumentasi
Peneliti melakukan pengumpulan data seperti foto, jurnal, buku, dokumen data anggota pegawai kementrian agama musirawas [12].

3. HASIL DAN PEMBAHASAN

Perkembangan dari berbagai macam serangan didunia maya saat ini menjadi sangat pesat dan semakin luas, serta makin banyaknya pengguna smartphone yang juga secara otomatis terkoneksi dengan internet, namun tidak diimbangi dengan tingkat pemahaman yang cukup untuk memilah dan memilih informasi maupun kegiatan bahkan tindakan kejahatan yang bisa terjadi melalui dunia maya dengan bermodalkan jejaring sosial yang saat ini melekat pada setiap orang. Selain itu dengan berkembangnya teknologi menjadikan tindak kejahatan yang tadinya dilakukan secara langsung melalui serangan berubah wujud nyata terhadap barang atau benda yang ada, kini serangan tindak kejahatan dapat dilakukan dengan metode jarak jauh dengan memanfaatkan media internet, guna mengumpulkan informasi target secara mendetail, salah satu cara yang digunakan adalah teknik phising.

Phishing pertama kali diperkenalkan pada tahun 1995. Menurut James (2005), cara pertama yang digunakan phisher adalah menggunakan algoritma yang menghasilkan nomor kartu kredit secara acak. Jumlah kartu kredit acak yang digunakan untuk membuat akun AOL[4]. Akun tersebut kemudian digunakan untuk mengirim spam ke pengguna lain dan untuk tujuan lain. Untuk menyederhanakan proses, program khusus seperti AOHell digunakan. Praktik ini diakhiri oleh AOL pada tahun 1995 ketika perusahaan menerapkan langkah-langkah keamanan untuk mencegah keberhasilan penggunaan nomor kartu kredit acak.

Phishing, juga dikenal sebagai "Brand Spoofing" atau "Carding", adalah bentuk layanan yang menyesatkan Anda dengan mengatakan bahwa data Anda legal dan aman. Menurut Felten et al (1997), spoofing dapat didefinisikan sebagai "teknik yang digunakan untuk mendapatkan akses tidak sah ke komputer atau informasi di mana penyerang berkomunikasi dengan pengguna berpura-pura menjadi tuan rumah yang terpercaya [4].

Phishing di layanan publik merupakan ancaman dengan menggunakan metode rekayasa sosial untuk menipu pengguna (pelanggan). Pengguna tertarik dengan penawaran melalui email, pesan singkat, panggilan telepon dari penjahat yang menyamar sebagai pejabat perusahaan. Masyarakat umum biasanya sering menyebut dengan phising. Istilah phishing berasal dari Bahasa inggris yaitu fishing (memancing). Phishing yaitu suatu bentuk penipuan yang dilakukan dengan cara

memalsukan data untuk mengelabui korban, tujuan dari phising yaitu agar mendapatkan informasi terhadap korban dari kata sandi sampai dengan kartu kredit, dengan cara menyamar menjadi orang atau bisnis yang terpercaya dalam suatu komunikasi elektronik resmi seperti surat elektronik atau pesan instan. Maka dari itu hal ini dinamakan memancing yang berarti memancing informasi keuangan dan kata sandi pengguna.

3.1. Cara Kerja Phishing

Dari definisi phishing, Anda dapat melihat bagaimana pekerjaan phishing dilakukan untuk memancing korban ke dalam jebakan phisher. Phishing adalah aktivitas seseorang untuk mendapatkan informasi sensitif pengguna menggunakan email dan situs web palsu yang terlihat seperti tampilan dan nuansa asli atau resmi dari situs web yang sebenarnya.

Phisher menggunakan email, spanduk, atau pop-up untuk mengelabui pengguna agar dialihkan ke halaman web palsu tempat pengguna diminta memberikan informasi pribadi. Di sinilah para phisher memanfaatkan ketidakpedulian dan ketidakpedulian pengguna jaringan palsu untuk mendapatkan informasi [4]. Berikut ini adalah aspek dari ancaman yang terinfeksi oleh virus phishing:

1) Manipulasi Tautan Beberapa metode phishing menggunakan manipulasi tautan agar terlihat seperti alamat institusi aslinya. Broken URL atau menggunakan subdomain adalah trik umum yang digunakan oleh phisher, seperti contoh URL di bawah ini: www.micosoft.com[4].
2) Filter Evasion Phisher menggunakan gambar (bukan teks) untuk memaksa pengguna mengungkapkan informasi pribadi mereka. Untuk alasan ini, Gmail atau Yahoo menonaktifkan gambar untuk email masuk secara default.[4]

Untuk membuat email phishing terlihat lebih asli, phisher/penipu memposting:

a) Tautan yang mengarah ke halaman web yang sah tetapi sebenarnya mengarah ke halaman web phishing.
b) Atau mungkin munculan yang persis seperti halaman resminya [4].

3.2. Cyber crime yang dilakukan oleh seorang phiser menggunakan beberapa teknik antara lain:

a) Email Spoofing
Teknik ini biasa digunakan phiser dengan cara mengirim email secara broadcast ke jutaan pengguna, seolah-olah berasal dari institusi resmi ang berisi seruan untuk melakukan sesuatu. Biasanya e-mail berisi pemintaan nomor kredit, password atau mengunggah form tertentu[5].
b) Pengiriman Berbasis Web
Pengiriman berbasis web adalah salah satu teknik phishing yang paling canggih. Dikenal sebagai “manin-the-middle”, phiser terletak diantara situs web asli dan sistem phishing [5].

c) Pesan Instan (chatting)
Olah pesan cepat adalah metode dimana pengguna menerima pesan berupa link yang diarahkan ke situs web palsu yang memiliki tampilan sama sehingga. pengguna merasa mengakses situs web resmi yang sah padahal palsu. [5]

d) Trojan hosts
Trojan hosts, phiser mencoba login ke account pengguna untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke phisher [5].

e) Manipulasi tautan (link)
Manipulasi link adalah teknik dimana phisher mengirimkan link ke sebuah website. Bila pengguna melakukan click pada link tersebut, maka akan diarahkan ke website phisher yang bukan link website sebenarnya.[5]

f) Malware Phishing
Penipuan yang melibatkan malware untuk dijalankan pada komputer pengguna. Malware ini biasanya melekat pada e-mail yang dikirimkan kepada pengguna oleh phisher. Setelah korban melakukan klik pada link, maka malware akan mulai berfungsi. Malware tersebut terkadang disertakan pada file yang dapat download [5].

3.3. Kasus pembobolan website Universitas Bina Insan Lubuklinggau dengan teknik phishing

Pada tahun 2022 terjadi kasus pembobolan website Universitas Bina Insan Lubuklinggau oleh seorang hacker yang tidak tau indetitasnya. Dimana hacker ini memanipulasi link ke sebuah website. Sehingga ketika Admin website Universitas Bina Insan mengklik tautan link tersebut maka data akun admin website Universitas Bina Insan terbaca oleh phisher. Sehingga phisher mendapatkan data akun admin website berupa username dan password admin website Universitas Bina Insan Lubuklinggau lalu seorang phisher merubah tampilan webiste Universitas Bina Insan Lubuklinggau dengan mengubah tampilan depan laman website Universitas Bina Insan Lubuklinggau, merubah tampilan menu-menu yang ada di website Universitas Bina Insan Lubuklinggau dan phiser juga melakukan pengambilan data-data yang ada di website universitas bina insan Lubuklinggau sehingga untuk mengatasi masalah tersebut depelover website Universitas Bina Insan Lubuklinggau merubah akun admin Universitas Bina Insan baik username dan passwordnya, lalu pihak depelover memperbaiki lagi kerusakan yang ada pada website Universitas Bina Insan Lubuklinggau. Merubah kembali tampilan depan yang di rusak oleh phisher, merubah menu-menu tampilan website yang di rusak oleh hacker, merestore data-data website Universitas Bina Insan yang hilang oleh phisher. Lalu dapelover tersebut membuat sistem firewall untuk lebih meningkat keamanan webiste Universitas Bina Insan Lubuklinggau.

3.4. Skenario kasus pembobolan website Universitas Bina Insan Lubuklinggau dengan teknik phishing.

Pelaku mengirim link situs palsu penyedia layanan hosting gratis dan menarik ke email admin website Universitas Bina Insan Lubuklinggau sehingga admin website Universitas Bina Insan Lubuklinggau mengklik link situs tersebut

saat bersamaan dengan adminstrator membuka akun admin website Universitas Bina Insan sehingga data akun usernme dan password admin website Universitas Bina Insan bisa terbaca oleh seorang phisher sehingga phisher dengan mudah menguasai website tersebut.

3.5. Dampak phishing website Universitas Bina Insna Lubulinggau

Danmpak phising terhadap website Universitas Bina Insan Lubuklinggau adalah website Universitas Bina Insan di ambil ahli oleh seorang phisher sehingga phisher dengan bebas melakukan apapun terhadap website Universitas Bina Insan. Phisher merubah tampilah halaman depan website Universitas Bina Insan, phisher juga merubah menu-menu pada website Universitas Bina Insan, phisher juga bisa mengambil data yang ada di website Universitas Bina Insan Lubuklinggau. Sehingga website Universitas Bina Insan Lubuklinggau di kuasai oleh phisher.

3.6. Cara mengatasi danmpak dari phishing terhadap website Universitas Bina Insan Lubuklinggau.

Ketika website Universitas Bina Insan Lubuklinggau berubah tampilan sehingga pihak dari administrator merasa bahwa website Universitas Bina Insan terkena hack dan administrator pun mencoba untuk mengakses akun admin website Universitas Bina Insan akan tetapi tidak bisa mengakses lagi akun admin website Universitas Bina Insan sehingga admin menghubungi developer atau pembuat website Universitas Bina Insan. Ketika mendapatkan pengaduan dari admin website Universitas Bina Insan developer langsung mengecek website Universitas Bina Insan Lubuklinggau, lalu developer menganalisa bahwa website Universitas Bina Insan terkena hack, dimana hacker menggunakan metode phishing untuk menjebak admin website Universitas Bina Insan, sehingga hacker bisa mendapatkan akun admin website Universitas Bina Insan Lubuklinggau untuk mengatasi masalah tersebut developer merubah username dan password admin Universitas Bina Insan sehingga hacker tidak bisa mengakses lagi akun admin website Universitas Bina Insan lalu pihak developer juga merubah lagi tampilan halaman website Universitas Bina Insan, baik tampilan halaman depan maupun halaman lain seperti tampilan semula. Developer juga memperbaiki lagi menu-menu website Universitas Bina Insan, sehingga menu-menu website Universitas Bina Insan bisa kembali seperti tampilan semula. Developer juga merestore data-data yang sempat di curi oleh hacker agar data website Universitas Bina Insan bisa kembali lagi. Developer juga memasang firewall terbaru untuk mengatasi serangan hacker ke website Universitas Bina Insan kedepanya.

3.7. Kasus phising pada website Digital Library Univrersitas Bina Insan Lubuklinggau

Pada tahun 2021 terjadi kasus phising pada website Digital Library dimana seorang phisher membuat website duplikat yang sama persis seperti website Digital Library Universitas Bina Insan Lubuklinggau, lalu seorang phisher menyebarkan link ke peguna website Digital Library Universitas Bina Insan, sehingga website Digital Library Universitas Bina Insan Lubuklinggau bisa di retas

dan di ambil ahli oleh phisher, ketika phisher bisa menguasai website Digital Library Universitas Bina Insan Lubuklinggau lalu phisher merubah tampilan website tersebut, baik tampilan depan, tampilan menu-menu website Digital Library dan tampilan yang lain pada website Digital Library Universitas Bina Insan.

3.8. Skenario kasus pembobolan website Digital Library Universitas Bina Insan Lubuklinggau dengan teknik phishing.

Seorang phisher membuat website duplikat yang hampir mirip seperti website Digital Library Universitas Bina Insan lalu menyebarkan link website duplikat tersebut ke pengguna Digital Library Universitas Bina Insan, ketika pengguna tersebut mengklik link yang diberikan oleh seorang phisher maka seorang phisher langsung bisa mendapatkan data-data pengguna tersebut dan bisa juga meretas website Digital Library Universitas Bina Insan yang asli.

3.9. Dampak phishing website Universitas Bina Insna Lubulinggau

Danmpak phising terhadap website Digital Library Universitas Bina Insan Lubuklinggau adalah website Digital Library Universitas Bina Insan di ambil ahli oleh seorang phisher sehingga phisher dengan bebas melakukan apapun terhadap website Universitas Bina Insan. Phisher merubah tampilah halaman depan website Digital Library Universitas Bina Insan, phisher juga merubah menu-menu pada website Digital Library Universitas Bina Insan dan merubah struktur website dari Digital Library Universitas Bina Insan serta admin dari website Digital Library tidak bisa login ke akun admin website itu lagi.

3.10. Cara mengatasi danmpak dari phishing terhadap website Universitas Bina Insan Lubuklinggau.

Ketika terjadi peretasan pada website Digital Library Universitas Bina Insan yang dilakukan oleh seorang phisher maka phisher dengan mudah menguasai website Digital Library Universitas Bina Insan tersebut. Lalu phisher merubah tampilan halaman depan website Digital Library Universitas Bina Insan, tampilan seacrh di website Universitas Bina Insan, tampilan menu-menu dari webiste Univeristas Bina Insan sehingga admin dari website tersebut tidak bisa lagi memegang kendali dari website Digital Library Universitas Bina Insan, untuk mengatasi hal tersebut pihak dari admin Digital Library Universitas Bina Insan menghubungi developer untuk melakukan perbaikan website Digital Library Universitas Bina Insan Lubuklinggau, lalu pihak Developer melakukan perbaikan dari website tersebut, dengan menutup akses seorang phisher untuk menguasai lagi website Digital Library Universitas Bina Insan, sehingga phisher tidak bisa lagi merubah ataupun menguasai webiste Digital Library Universitas Bina Insan lalu developer memperbaiki tampilan website Digital Library Universitas Bina Insan dan memasang firewall agar tidak mudah di retas oleh seorang hacker maupun phisher.

4. SIMPULAN

Dari penulisan maka dapat disimpulkan beberapa hal bahwa seorang phisher melakukan peretasan dengan cara membuat website duplikat lalu menyebarkan link ke pengguna website yang asli sehingga ketika pengguna website yang asli tersebut mengklik link tersebut maka seorang phisher dengan mudah mencuri data-data dari pengguna website yang asli. Tidak hanya data dari pengguna asli seorang phisher juga bisa menguasai website yang asli tersebut. Phishing adalah aktivitas cyber crime yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data identitas dan kredensial akun keuangan. Phishing merupakan tidak kejahatan cyber yang sangat merugikan korbanya karna semua data korban bisa dicuri oleh phisher.

DAFTAR PUSTAKA

[1] N. Widya Ramailis, "Cyber Crime Dan Potensi Munculnya Viktimisasi Perempuan Di Era Teknologi Industri 4.0," *Sisi Lain Realita*, vol. 5, no. 01, pp. 1–20, 2020, doi: 10.25299/sisilainrealita.2020.vol5(01).6381.

[2] A. R. Kelrey and A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 2, pp. 77–81, 2019, doi: 10.14421/csecurity.2019.2.2.1625.

[3] B. Suharto and A. B. Kurniawan, "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising)," *JHP 17 (Jurnal Has. Penelitian)*, vol. 5, no. 2, pp. 57–61, 2020, [Online]. Available: http://jurnal.untag-sby.ac.id/index.php/jhp17

[4] Muftiadi A, Putri Mulyani Agustina T, and Evi M, "Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking," *J. Ilm. Tek.*, vol. 1, no. No. 2, Agustus 2022, pp. 60–65, 2022.

[5] Z. Efendy, I. E. Putra, and R. Saputra, "Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process," *J. Terap. Teknol. Inf.*, vol. 2, no. 2, pp. 135–146, 2019, doi: 10.21460/jutei.2018.22.103.

[6] W. Candraditya Pamungkas and F. Trimuti Saputra, "Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling," *J. Ris. Komputer)*, vol. 7, no. 4, pp. 2407–389, 2020, doi: 10.30865/jurikom.v7i4.2304.

[7] T. Rompi and H. S. Muaja, "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan," *Lex Priv.*, vol. IX, no. 4, pp. 183–192, 2021, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358

[8] D. Irawan, "Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising," *JIKI (Jurnal llmu Komput. lnformatika)*, vol. 1, no. 1, pp. 43–46, 2020, doi: 10.24127/jiki.v1i1.671.

[9] D. N. Hidayat, "Metodologi Penelitian dalam Sebuah Multi-Paradigm Science," *Mediat. J. Komun.*, vol. 3, no. 2, pp. 197–220, 2002.

[10] M. R. Fadli, "Memahami desain metode penelitian kualitatif," *Humanika*, vol. 21, no. 1, pp. 33–54, 2021, doi: 10.21831/hum.v21i1.38075.

[11] R. S. P. Selfi Fitria Sari, "Literature Review Sistem Pengelolaan Arsip Di Kantor Kelurahan Keboledan Kecamatan Wanasari Kabupaten Brebes," *J. Ekon. dan Akunt.*, vol. 2, no. 1, pp. 116–126, 2022.