LITE: Jurnal Bahasa, Sastra, dan Budaya
ISSN online: 2548-9588 ISSN print.: 1907-3607
https://publikasi.dinus.ac.id/index.php/lite
Published by Universitas Dian Nuswantoro, Semarang

The form and meaning of language motifs in phishing crimes: A forensic linguistic study

Zahy Riswahyudha Ariyanto, Laili Etika Rahmawati*
Universitas Muhammadiyah Surakarta, Jl. A. Yani, Sukoharjo, Indonesia

Article History

Submitted date:
2024-09-02
Accepted date:
2025-03-30
Published date:
2025-04-10

Keywords:

cybercrime; forensic linguistics; language motifs; phishing

Abstract

This research aims to describe the form and meaning of the language used in phishing actions from a forensic linguistics perspective. This research is qualitative research with descriptive methods. The data in this research is text transcriptions of messages and information indicated in phishing crimes. Research stages include (1) data documentation, (2) data classification, (3) data analysis, (4) interpretation of form and meaning based on a forensic linguistic perspective, and (5) data conclusion. The data in this research are messages or information in phishing actions. The data sources in this research come from social media, digital forums, and social media, often a means of cyber-crime, such as WhatsApp, Facebook, and Twitter. Data collection techniques use documentation techniques. The data validity test was carried out using theoretical triangulation. The data analysis technique uses discourse analysis; researchers identify language patterns used in phishing crime communications. The results of this research show that the forms of language motives in phishing crimes include (1) 10 deceptive phishing, 4 Phishing APKs, and 6 smishing. and the meaning of language motifs in phishing crimes. This research concludes that there are various types of phishing crimes packaged in persuasive and manipulative language. In this research, forms of phishing action have been found, including deceptive phishing, APK phishing, and smishing, and the meaning of language motifs in phishing actions has been identified.

Kata Kunci:

kejahatan siber; linguistik forensik; motif bahasa; phishing

Abstrak

Bentuk dan makna motif bahasa dalam aksi kejahatan *phishing*: Kajian linguistik forensik

Penelitian ini bertujuan untuk mendeskripsikan bentuk dan makna bahasa yang digunakan dalam aksi *phishing* berdasarkan perspektif linguistik forensik. Penelitian ini merupakan jenis kualitatif dengan metode deskriptif. Data penelitian ini berupa transkripsi teks dari pesan dan informasi yang terindikasi dalam kejahatan *phishing*. Tahapan penelitian meliputi: (1) pendokumentasian data; (2) klasifikasi data; (3) analisis data; (4) penafsiran bentuk dan makna berdasarkan perspektif linguistik forensik; dan (4) penyimpulan data. Data dalam penelitian ini adalah pesan atau informasi dalam aksi *phishing.* Sumber data dalam penelitian ini berasal dari media sosial dan forum digital dan media sosial yang sering menjadi sarana kejahatan siber seperti *whatsapp, facebook, twitter*. Teknik pengumpulan data menggunakan teknik dokumentasi. Uji keabsahan data dilakukan menggunakan triangulasi teori. Teknik analisis data menggunakan analisis wacana, peneliti mengidentifikasi pola-pola bahasa yang digunakan dalam komunikasi kejahatan *phishing.* Hasil penelitian ini menunjukkan bahwa bentuk-bentuk motif bahasa dalam aksi kejahatan *phishing* di antaranya 10 *deceptive phishing*; 4 *Phishing* APK; (6) *smishing*. dan makna motif bahasa dalam aksi kejahatan *phishing.* Simpulan penelitian ini bahwa terdapat beragam jenis kejahatan *phishing* yang dikemas dengan bahasa persuasif dan manipulatif, dalam penelitian ini telah ditemukan bentuk-bentuk aksi *phishing* di antaranya (1) *deceptive phishing*; *phishing* APK; *smishing*, serta telah diidentifikasi makna motif bahasa dalam aksi *phishing*.

* Corresponding author:
laili.rahmawati@ums.ac.id

1 Pendahuluan

Penipuan *online* telah menjadi fenomena yang semakin marak terjadi di era digital saat ini. Kemajuan teknologi dan perangkat elektronik memudahkan akses internet bagi masyarakat dari berbagai kalangan. Adanya akses internet yang lebih luas menjadikan berbagai kalangan, dari anak-anak hingga orang dewasa dapat menggunakan internet untuk berbagai tujuan (Strada dkk., 2022). Namun, kemudahan dalam mengakses internet juga membuka peluang bagi tindak kriminal seperti penipuan *online* (Kemp dkk., 2021). Penipuan *online* sebenarnya mirip dengan penipuan konvensional, namun dilakukan melalui media elektronik (Purba & Can, 2016). Hal ini membuat pelaku penipuan lebih sulit dilacak dan diidentifikasi, sehingga banyak kasus yang tidak terungkap. Pada tahun 2024, kejahatan *phishing* terus menjadi ancaman signifikan dalam dunia siber. Berdasarkan laporan terbaru, *phishing* mencakup sekitar 39,6% dari semua ancaman email. Hampir 96% organisasi melaporkan setidaknya satu serangan *phishing* dalam setahun terakhir, dengan 52% menganggap ancaman ini semakin canggih (AAG IT Support, 2024). Puspitasari (2018) menyatakan bahwa secara hukum, penipuan *online* diakui sebagai tindak kriminal yang dapat merugikan orang lain. Tindakan ini diatur dalam hukum pidana, dan pelakunya dapat dikenakan sanksi yang jelas. Penipuan *online* dikemas melalui pesan dan informasi yang mengandung bahasa persuasif dan manipulatif untuk menjebak korban.

Kejahatan yang menggunakan bahasa sebagai alat untuk merugikan orang lain semakin sering terjadi di Indonesia (Warami, 2022). Jenis kejahatan ini meliputi berbagai bentuk manipulasi verbal seperti ujaran kebencian, penyebaran hoaks, hasutan, teori konspirasi, sumpah palsu, ancaman, dan penyuapan (Taufiq dkk., 2023). Kejahatan berbahasa menjadi ancaman serius bagi masyarakat karena dapat menyebabkan kerugian dan rasa tidak aman (Napitupulu, 2017). Fenomena ini timbul akibat kemajuan teknologi informasi dan rendahnya tingkat literasi di Indonesia, yang membuat masyarakat sering kurang cermat dalam memahami informasi dari berbagai media (Fitriarti, 2019). Menurut Grecya dkk., (2021) Indonesia masih tertinggal dalam penerapan pendekatan sistemik untuk melawan disinformasi. Rendahnya budaya literasi di Indonesia membuat masyarakat mudah terpengaruh oleh informasi yang salah atau menyesatkan (Sabina dkk., 2023). Oleh karena itu, upaya untuk meningkatkan literasi digital dan kemampuan masyarakat dalam menyaring informasi sangat penting. Selain itu, diperlukan kebijakan yang lebih tegas dan komprehensif untuk menindak pelaku kejahatan berbahasa serta edukasi berkelanjutan agar masyarakat lebih kritis dalam menerima informasi dari berbagai sumber.

Penggunaan pesan di media sosial atau *platform* komunikasi lainnya untuk merayu atau menipu individu agar melakukan tindakan tertentu yang membuka peluang bagi pelaku untuk melakukan kejahatan siber (Dearden dkk., 2023). Manipulasi bahasa menjadi alat bagi pelaku untuk mencapai tujuannya (Saifudin, 2024), yaitu memperoleh informasi sensitif atau akses ilegal ke data pribadi korban. Pelaku menggunakan bahasa persuasif dan manipulatif menciptakan ilusi kepercayaan dan memanipulasi korban agar melakukan tindakan yang menguntungkan pelaku kejahatan (Putri, 2022). Kejahatan siber hadir dalam berbagai bentuk, salah satunya yang marak terjadi adalah *Phishing*. *Phising* adalah ancaman yang menggunakan teknik rekayasa sosial yang mengelabui pengguna dengan meniru identitas entitas yang berwenang (Karamagi & Ally, 2023). *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. *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 (Caniago & Sutabri, 2023). *Phisher* menggunakan email, pesan, 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 (Muftiadi dkk., 2022).

Menurut Lokapala dkk (2024) kejahatan *phishing* terjadi akibat kurangnya kesadaran dan pengetahuan masyarakat dalam melindungi diri, sehingga mereka menjadi mudah menjadi korban. Selain itu, keterbatasan sumber daya manusia yang profesional dan berkualifikasi khusus untuk mendeteksi kejahatan *phishing* juga menjadi faktor penyebab. Keterbatasan teknologi yang ada membuat pelaku lebih mudah melancarkan aksi dengan teknik kamuflase yang canggih. Lebih lanjut, kejahatan *phishing* dapat melibatkan yurisdiksi dari beberapa negara, yang memperumit proses penegakan hukum, terutama dalam hal pengumpulan bukti digital. Maka, penelitian ini sebagai jawaban atas permasalahan tersebut. Solusi atas kebutuhan yaitu identifikasi motif bahasa dalam aksi kejahatan *phishing* sebagai upaya preventif serta edukasi masyarakat mengenai bahaya *phishing*. Kajian terhadap pola komunikasi yang digunakan oleh pelaku sebagai pengembagan strategi yang lebih efektif untuk mendeteksi dan mencegah upaya *phishing* yang dibungkus dengan pesan dan informasi persuasif dan manipulatif. Nugroho dkk (2023) perlu segera dimasifkan edukasi kepada masyarakat mengenai ciri-ciri pesan *phishing* dan percepatan pengabdian tentang literasi digital akan meningkatkan kesadaran dan kewaspadaan masyarakat, sehingga lebih mampu melindungi diri dari ancaman *phishing* yang kompleks tersebut.

Berdasarkan fenomena maraknya kejahatan *phishing*, urgensi yang dihadapi saat ini adalah upaya preventif untuk menghadapi serangan *phishing*. Salah satu aspek yang harus menjadi fokus adalah identifikasi tentang kejahatan siber yang dibungkus dengan bahasa persuasif dan manipulatif (Amro, 2018). Pelaku *phishing* menggunakan teknik komunikasi yang sangat meyakinkan untuk menjebak dan mempengaruhi calon korban. Pelaku memanfaatkan kelemahan psikologis korban, dengan membangun rasa percaya melalui pesan yang terlihat sah dan kredibel (Kothamasu dkk., 2023). Adapun tindakan yang dilakukan, seperti pelaku dapat mengirim email atau pesan yang tampak berasal dari sumber yang terpercaya, meminta korban untuk membuka tautan atau memberikan informasi pribadi (Dharani dkk., 2024). Penggunaan bahasa yang meyakinkan dan manipulatif ini membuat korban secara tidak sadar mengikuti perintah pelaku, yang akhirnya mengarah pada pelepasan informasi pribadi secara sengaja.

Kajian mengenai bentuk dan makna motif bahasa dalam aksi kejahatan *phishing* memiliki urgensi yang sangat tinggi, karena bahasa merupakan alat utama yang digunakan oleh pelaku untuk menjebak dan memanipulasi korban. Bahasa persuasif dan manipulatif dalam *phishing* dirancang untuk menciptakan ilusi kepercayaan dan mendorong korban mengambil tindakan tertentu tanpa berpikir panjang. Melalui telaah struktur dan strategi bahasa yang digunakan dalam pesan *phishing*, dapat diidentifikasi pola-pola komunikasi yang khas dari kejahatan ini. Kajian linguistik terhadap *phishing* membuka pemahaman yang mendalam mengenai bagaimana bahasa dipakai sebagai sarana penipuan digital yang efektif.

Dalam kerangka teoretis, penelitian ini menggunakan pendekatan linguistik forensik, yaitu cabang ilmu linguistik yang mengkaji penggunaan bahasa dalam konteks hukum dan kriminal. Menurut Lwin Tun & Birks (2023), linguistik forensik mencakup penerapan teori dan metode linguistik pada situasi hukum di mana bahasa berperan sebagai bukti atau alat kejahatan. Kajian ini mencakup analisis teks tertulis, lisan, maupun digital, yang sering digunakan dalam tindak pidana, termasuk penipuan berbasis pesan elektronik seperti *phishing*. Linguistik forensik berperan penting dalam kerja lintas disiplin yang melibatkan ahli bahasa, penyelidik, penegak hukum, hingga pengacara, guna mengungkap makna tersembunyi, motif pelaku, dan dampak linguistik terhadap korban.

Hasil kajian ini diharapkan mampu berkontribusi dalam pengembangan metode identifikasi *phishing* berbasis bahasa serta perancangan program edukasi publik yang lebih efektif. Pemahaman atas teknik komunikasi pelaku dapat digunakan untuk meningkatkan akurasi sistem pendeteksi otomatis (seperti filter *spam* dan *anti-phishing*), serta memperkuat strategi kampanye literasi digital. Seiring meningkatnya kompleksitas taktik *social engineering*, edukasi berbasis *critical thinking* dalam membaca pesan digital menjadi kunci dalam mencegah kerugian akibat kejahatan siber (Dharani dkk., 2024). Oleh karena itu, penguatan kapasitas linguistik masyarakat perlu dikedepankan sebagai bentuk pertahanan awal terhadap serangan digital berbasis manipulasi bahasa.

Penelitian terdahulu mengenai identifikasi kejahatan *phishing* sebagian besar berfokus pada aspek teknis dan pemodelan sistem. Misalnya, Weaver dkk. (2021) meneliti efektivitas pelatihan singkat dalam meningkatkan kemampuan pengguna dalam membedakan *phishing* dan email sah, sedangkan Lin dkk. (2021) mengembangkan sistem *Phishpedia* berbasis *deep learning* untuk mendeteksi logo dan variasi visual pada halaman web *phishing*. Sementara itu, Orunsolu dkk. (2022) mengembangkan model prediktif berbasis pembelajaran mesin untuk meningkatkan efisiensi sistem deteksi otomatis. Penelitian-penelitian tersebut menekankan aspek visual dan sistem kecerdasan buatan sebagai alat utama mitigasi.

Namun, kajian mengenai dimensi linguistik, khususnya motif bahasa dalam pesan *phishing*, masih jarang disentuh secara mendalam dalam ranah akademik sehingga menciptakan celah penelitian yang signifikan. Inilah yang menjadi fokus utama dan keunikan dari studi ini, yaitu dengan menghadirkan pendekatan linguistik forensik untuk mengidentifikasi dan mengungkap bentuk serta makna bahasa dalam aksi *phishing*. Pendekatan ini memberikan perspektif baru yang melengkapi dominasi pendekatan teknis sebelumnya yang lebih berorientasi pada aspek sistem keamanan atau pemrograman. Dengan menganalisis secara sistematis unsur-unsur linguistik seperti pilihan diksi, struktur kalimat, gaya bahasa, dan tindak tutur (*speech act*), penelitian ini menawarkan model identifikasi berbasis bahasa yang lebih humanistik dan kontekstual. Signifikansi dari penelitian ini terletak pada kontribusinya terhadap pengembangan strategi mitigasi kejahatan digital yang lebih komprehensif, melalui peningkatan literasi linguistik digital masyarakat dan pendeteksian dini terhadap potensi *phishing* melalui motif kebahasaan yang khas.

2 Metode

Jenis penelitian ini adalah penelitian kualitatif dengan metode deskriptif. Penelitian ini menggunakan metode deskriptif kualitatif, sesuai dengan data yang digunakan dalam penelitian ini yaitu data deskripsi yang berupa transkripsi teks dari pesan dan informasi yang terindikasi dalam aksi *phishing.* Data dalam penelitian ini adalah data teks dari data-data dokumentasi tangkapan layar pesan atau informasi yang termasuk upaya kejahatan *phishing.* Sumber data dalam penelitian ini berasal dari media sosial dan forum digital yang sering menjadi sarana kejahatan siber, seperti Facebook, Twitter, Situs Web, dan layanan SMS.

Adapun langkah-langkah dalam penelitian ini sebagai berikut. Pertama, peneliti melakukan proses dokumentasi data dari berbagai platform media sosial seperti Facebook, Twitter, Situs Web dan layanan SMS, khususnya menangkap pesan atau informasi yang dicurigai sebagai *phishing* dengan menggunakan tangkapan layar. Kedua, data yang terdokumentasi kemudian diklasifikasikan berdasarkan jenis *phishing* dan karakteristik pesan *phishing* untuk memudahkan analisis lebih lanjut. Ketiga, analisis dilakukan dengan teknik analisis wacana dan kerangka kerja linguistik forensik untuk mengungkap pola-pola bahasa yang digunakan dalam komunikasi *phishing.* Pola-pola bahasa yang diidentifikasi meliputi penggunaan kata-kata manipulatif seperti "*hadiah gratis", "verifikasi akun segera"*, dan *"akses terbatas"*; strategi intimidasi seperti ancaman pemblokiran akun atau denda; serta janji-janji palsu yang bertujuan untuk membujuk korban agar memberikan informasi pribadi.

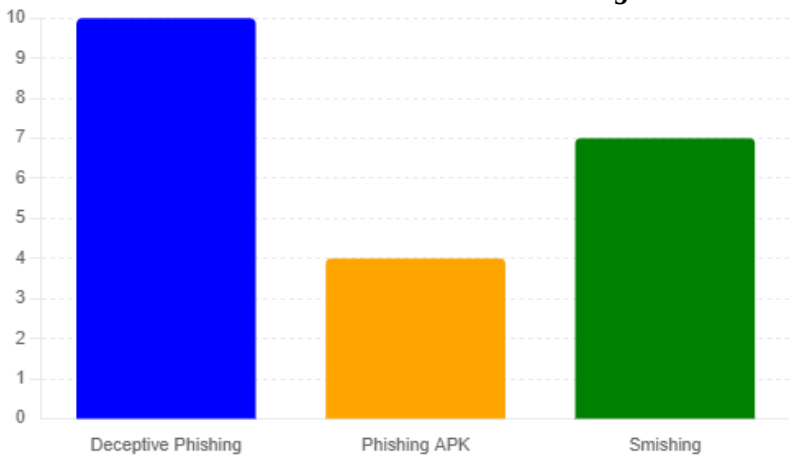
Keempat, penafsiran bentuk dan makna dilakukan menggunakan perspektif linguistik forensik untuk memahami bagaimana pesan tersebut memanipulasi bahasa untuk menipu korban. Kelima, peneliti kemudian menyimpulkan temuan-temuan berdasarkan analisis data, merangkum strategi manipulatif yang digunakan dalam pesan *phishing* untuk memperingatkan dan melindungi pengguna dari ancaman kejahatan siber tersebut.

Teknik pengumpulan data dalam penelitian ini adalah teknik dokumentasi. Apabila ditemukan pesan atau informasi yang terindikasi dalam kejahatan *phishing*, peneliti melakukan dokumentasi *screenshot* guna menyimpan data tersebut dan melakukan kajian terhadap data tersebut. Uji keabsahan data menggunakan triangulasi. Secara spesifik menggunakan triangulasi teori dengan memakai lebih dari satu teori atau kerangka konseptual untuk menganalisis fenomena dalam penelitian ini. Peneliti menggunakan teori analisis wacana, teori semantik, dan teori kriminologi bahasa untuk menganalisis bentuk dan makna bahasa yang digunakan dalam aksi kejahatan siber. Selain itu, teori tindak tutur (*speech act theory*) digunakan untuk memahami bagaimana tindakan ujaran dalam pesan *phishing* mempengaruhi dan mengarahkan korban. Teknik analisis data menggunakan analisis wacana. Peneliti mengidentifikasi pola-pola bahasa yang digunakan dalam komunikasi kejahatan *phishing*, termasuk strategi manipulasi, penipuan, atau intimidasi. Kerangka kerja linguistik forensik digunakan seperti analisis fitur linguistik, struktur wacana, dan konvensi komunikatif untuk mengeksplorasi hubungan antara bahasa dan tindakan kejahatan *phishing.*

3 Hasil

Phishing diklasifikasikan menjadi beberapa jenis, utamanya ada 3 di antaranya adalah Deceptive Phishing, Phishing *APK*, dan Smishing (Anggana, 2024). Penelitian ini mengidentifikasi tiga jenis utama kejahatan phishing, yaitu Deceptive Phishing, Phishing *APK*, dan Smishing. Deceptive Phishing melibatkan penipuan melalui tampilan dan bahasa yang menyerupai komunikasi resmi untuk mencuri informasi pribadi. Phishing *APK* menggunakan aplikasi berbahaya (APK) yang diunduh oleh korban untuk menginfeksi perangkat mereka. *Smishing* memanfaatkan pesan teks atau *Whatsapp* untuk menipu dan mengeksploitasi korban dengan tautan atau informasi palsu. Berdasarkan penelitian yang telah dilakukan, ditemukan 10 data *Deceptive Phishing*, 4 data *Phishing* APK, dan 7 data *Smishing.*

Gambar 1 Temuan Klasifikasi Data *Phishing*



Tabel 1 Data Deceptive Phishing

No Data	Data	Sumber	Keterangan
01	PERINGATAN!! Kami dari pihak *Facebook* memperingati bahwa *Facebook* anda sedang bermasalah.harap verifikasi akun anda sebelum akun anda dinonaktifkan demi keamanan.Di karenakan seseorang telah melaporkan akun anda, memiliki konten yang tidak pantas dan berkata kasar. Untuk melanjutkan kembali akun anda. https://veriifiikasii-blokir.weebly.com/ pemulihan-xxxxx Catatan: Jika anda membatalkan pemblokiran maka fecebook anda akan dinonaktifkan tanpa pemberitahuan lagi harap verifikasi secepatnya Terima kasih atas bantuan Anda untuk meningkatkan layanan kami. Kami sangat menyesal atas ketidaknyamanan ini	Facebook	Informasi Mengatasnamakan Pihak *Facebook*
02	Halo @boy_delivery_kediri Telah ditentukan bahwa akun Anda adalah penghasil konten yang bermanfaat bagi komunitas dan telah diputuskan bahwa akun Anda akan menerima lencana biru, Isi form berikut dengan benar: https://shrt-n.*online*/www .*instagram*.com/ig/?id= 798dxxxxxx Setelah itu tim dukungan *Instagram* akan menghubungi Anda, isi formulir dengan lengkap dan benar untuk melalui, jika tidak proses penambahan lencana akan gagal.	Instagram	Pesan Mengatasnamakan Pihak *Instagram*
03	Bagi yang sudah memiliki E-KTP sudah bisa mengambil kompensasi Per Tgl 29 agustus 2021 sebesar Rp. 600.000 untuk biaya # dirumah aja. Silakan cek apakah nama anda tercantum, dan cocokkan dengan NIK E-KTP anda melalui link benikut https//bit.ly/3zPxxxxx	Website Palsu	Informasi Mengatasnamakan Dinas Sosial
04	Selamat pagi teman, saya cuma mau ngasi informasi penting, jne lagi bagi2 hadiah samsung s7, cuma dengan modal 100ribu pulsa, awalnya sih ragu setelah saya cobain ternyata beneran dapat samsung s7 rezeki gk kemana ya buruan cobain ini situs nya: ptjne.cxxxxx	Facebook (Akun Dickaxxx)	Pesan yang Mengatasnamakan Pihak JNE
05	GIVE AWAY BAIM PAULA #Selamat Untuk pemenang Sesi 4 Spam p 10 20jt Spam p 20= 40jt Spam p 3060jt Spam p 40 100jt SILAHKAN KLIK AMBIL HADIAH DISINI https://linktr.ee/Giveawayrexxxxx NB.TANPA DI PUNGUT BIAYA ŞEPESERPUN ~SAYA PILIH YANG PALING BANYAK SPAM (P) WAJIB SHARE KE 3 GRUB	Akun Facebook Baim Wong (Palsu)	Pesan Mengatasnamakan Artis Terkenal
06	*Facebook* Anda Memiliki Konten Yang Tidak Pantas Atau Berkata Kasar Dan Aktivitas Anda Tidak Mengikuti Standar Komunitas *Facebook*. Apabila Anda Merasa Tuduhan Ini Adalah Salah Dan Tidak Benar. Silahkan Konfirmasi *Facebook* Anda Untuk Melakukan Pembatalan Pemblokiran Dan Untuk Menunjukan Bahwa Anda Benar Benar Pemilik Asli *Facebook* Tersebut : Cara / Langkah Untuk *Facebook* Anda, Membatalkan Pemblokiran Silahkan Klik Tautan Di Lengkapi Data Data Anda ah in Dan Dengan Benar. tautan inights amantacebook2021.weexxxxx	Facebook	Informasi Mengatasnamakan *Facebook*

No Data	Data	Sumber	Keterangan
	Apabila Tidak Membatalkan Pemblokiran, *Facebook* Anda Akan Di Non Aktifkan Tanpa Pemberitahuan Lagi		
07	Hai, nama saya Diana, dan saya bekerja di departemen pemasaran *Tokopedia* (cabang Indonesia). Pengguna *Tokopedia* yang terhormat, selamat menjadi pengguna yang beruntung, Anda akan mendapatkan penanak nasi Philips senilai Rp 1.000.000 secara gratis Gratis, tanpa biaya, dan pengiriman gratis! Klik tautan untuk menambahkan layanan pelanggan aktif untuk menerima *whatsapp*: Whatapp.mxxxxx	+6277356xxxx (Mengatasnamakan *Tokopedia*)	+6277356xxxx (Mengatasnamakan *Tokopedia*)
08	POS INDONESIA Pelanggan yang terhormat Paket Anda tidak dapat dikirim pada 01.07.2021 masuk yang dibayarkan (5648.99 Rp) karena tidak ada bea Pedagang: Ems Pos Indonesia Jumlah order: ID-14237325-1 Jumlah pembelian: 5648.99 Rp Untuk mengkonfirmasi paket Anda Klik disini. Anda akan menerima Email atau SMS ketika Anda tiba di alamat rumah Anda. Anda akan memiliki 8 hari, dari tanggal ketersediaan, untuk menarik paket. Setelah penarikan anda akan dimintai ID. Terima kasih.	Email Pos Indonesa (Palsu)	Email Mengatasnamakan POS Indonesia
09	Saya adalah agen *Tiktok*, dan saat ini kami sedang mencari mitra untuk bergabung dengan tim kami. Berdasarkan data konten dan komentar Anda, kami yakin Anda sangat cocok untuk bergabung dengan agensi *Tiktok* kami. Cukup ikuti petunjuk untuk membuat toko *Tiktok* Anda di platform kami. Tanpa perlu pengalaman., Anda akan mendapatkan bimbingan satu per satu dari tutor kam. Kami menjamin pendapatan stabil minimal 300.000 IDR per hari. Jika Anda berminat (usia 24+), silakan hubungi tutor kami melalui *Whatsapp* dan lampirkan tangkapan layar undangan ini. *Whatsapp*: https://watiktoxxxxx	Whatsapp (Agen TikTok Palsu)	Pesan Mengatasnamakan Pihak *Tiktok*
10	Nasabah bank BRI Yang terhormat Untuk komfirmasi Tarif Transaksi anda silahkan klik di bawah ini Terimakasi http:/perubahantarifbri6500. Silakan di klik link yang telah kami sediakan ya bapak/ibu dan itu akan langsung mengarahkan bapak/íbu kek formulir untuk pengaktifan tarif nya Jika sudah di isi tolong konfirmasi lagi ke kami	Whatsapp (CS BRI Palsu)	Pesan Mengatasnamakan Instansi BRI

Tabel 2 Data *Phishing APK*

No Data	Data	Sumber	Keterangan
11	A: Surat Undangan Pernikahan Digital.apk 6,6 MB A: Kami harap kehadiran nya B: Ini siapa..... A: Silahkan di buka agar lebih jelas dan kenal kk B: Bpk salah kirim.....	08121347xxxx (Whatsapp)	Undangan APK
12	A: Assalamualaikum kak selamat siang kak, Ada paket B: Ok taruh saja di dalem A: Cek Resi Paket JNT (apk)	081990785xxx (Whatsapp)	Resi JNT APK

No Data	Data	Sumber	Keterangan
	Konfirmasi		
13	Selamat siang pak/ibu Kami dari kepolisian menginformasikan bahwa bapak/ ibu melakukan pelanggaran, Silakan Buka aplikasi untuk melihat surat tilangnya Jika suratnya sudah dibaca silakan segera datang ke kantor polisi yang terdekat (Surat Tilang-1.0.apk)	08211189xxxx (Whatsapp)	Surat Tilang APK
14	A: Selamat siang kak Benar dengan SALMAH Ada Paket di J&T Express Nama SALMAH (LIHAT Foto Paket APK) B: Ada Paket d. J&T Express Nama SALNAH paket ap?	08595065xxxx (Whatsapp)	Foto Paket J&T APK

Tabel 3 Data *Smishing*

No Data	Data	Sumber	Keterangan
15	Dapatkan bantuan sebesar 600.000 dari pemerintah lewat program prakerja Kartu Prakerja adalah program pengembangan kompetensi berupa bantuan biaya yang ditujukan untuk pencari kerja, pekerja ter-PHK atau pekerja yang membutuhkan peningkatan kompetensi. Bantuan akan dikirim setiap bulan selama program ini berjalan Langkah untuk mendaftar Prakerja Kunjungi situs web di bawah ini Isi formulir data diri Anda akan mendapatkan pemberitahuan melalui email/nomor hp Bantuan akan dikirim melalui rekening bank harap bagikan pesan ini kepada kerab yang membutuhkan http://vip-09.fit/j/xxxxx	08214276xxx (Whatsapp)	Informasi Kartu Prakerja
16	Organisasi Kesehatan Dunia Untuk merayakan hari jadi kami yang ke 10, kami memberikan 1000 G... *Whatsapp* menawarkan internet 1000 GB Anda sekarang bisa mendapatkan paket internet gratis 50GB (Semua Jaringan) berlaku selama 90 hari di Perayaan Ulang Tahun *Whatsapp*. Saya Telah Menerima Punyaku Cepat sebelum Habis https://asvip1.top/j/5xxxxx	Pesan Berantai Whatsapp	Pesan Berantai WHO Palsu
17	Code *Whatsapp* Anda [676898] Dapatkan Rp,75.000.000,U/Info klik.https://bit.ly/2Nxxxxx	SMS Kode	Pesan Kode Verifikasi *Whatsapp*
18	N.O.Anda dpt Rp.100.000.000 program dri memberikan KEDAS BE4UTY tahun 2021 kode pin (CK805KU) silahkan cocokkan pin anda di; bit.ly/infogiveaxxxxx	085879554xxx (SMS)	Pesan Berantai Iming-Iming Hadiah Uang
19	Anda Menerima D4n4 B4ntu4n D4ri Kanotr Pusat untuk info bit.ly/Bpjsindonexxxxx	085295310xxx (SMS)	Pesan berantai Bantuan BPJS
20	UNICEF - Subsidi pemerintah Melalui kuesioner, Anda akan memiliki kesempatan untuk mendapatkan Rp11.831.200. http://luckybreakthrough.buzz/BtwJob /xxxxxx	Pesan berantai Unicef Palsu (SMS)	Pesan Permohonan Mengisi Kuesioner Unicef Palsu
21	aman! Pinjaman Rp 20.000.000 yang Anda ajukan telah disetujul, silakan klik tautan untuk mengonfimasi pinjaman. https:/www.idnsloxxxx	Pesan Berantai Pinjaman *Online*	Pesan Berantai Tawaran Pinjaman *Online*

Berdasarkan temuan data kejahatan berbahasa dalam konteks *phishing*, seluruh pesan telah diklasifikasikan ke dalam tiga jenis utama *phishing*, yaitu *deceptive phishing*, *phishing APK*, dan *smishing*. Klasifikasi ini menjadi dasar untuk menganalisis lebih lanjut bentuk dan makna motif bahasa yang digunakan oleh pelaku dalam setiap jenis serangan. Analisis dilakukan dengan pendekatan linguistik forensik, secara khusus menyoroti aspek konteks wacana dan pragmatik, guna mengungkap strategi manipulatif dan maksud tersembunyi dalam pesan-pesan tersebut.

4. Pembahasan

Berdasarkan kajian yang telah dilakukan peneliti mengungkap motif bahasa persuasif dan manipulatif digunakan oleh pelaku dalam aksi kejahatan siber. Peneliti menemukan motif bahasa dalam berbagai kasus *phishing*, ditemukan fakta bahwa pelaku secara sistematis menggunakan strategi komunikasi yang dirancang untuk membangun rasa percaya, menggiring persepsi korban, dan memanipulasi tindakan korban agar memberikan masuk ke sebuah tautan. Bahasa yang digunakan dalam kejahatan *phishing* mengandung unsur-unsur yang dirancang untuk menciptakan ilusi kepercayaan, seakan-akan berasal dari instansi resmi. Pelaku menggunakan istilah-istilah teknis, gaya bahasa formal, dan elemen-elemen visual seperti logo dan tanda tangan elektronik yang menyerupai lembaga atau organisasi terpercaya. Hal ini bertujuan untuk meyakinkan korban bahwa permintaan informasi tersebut sah dan harus segera ditindaklanjuti. Selain itu, pelaku sering kali menggunakan tekanan waktu atau ancaman implisit untuk mendorong korban bertindak cepat tanpa berpikir panjang.

Analisis linguistik forensik dilakukan guna mengidentifikasi pola-pola bahasa yang secara khusus dirancang untuk memanfaatkan kondisi-kondisi ini, menunjukkan betapa canggihnya teknik manipulasi yang digunakan. Pembahasan ini mengungkapkan bentuk dan makna bahasa dalam aksi *phishing* sebagai upaya preventif yang terfokus pada peningkatan literasi digital dan kesadaran tentang taktik manipulatif yang digunakan dalam kejahatan siber. Adapun jenis-jenis *phishing* yang ditemukan adalah *smishing*, *deceptive phishing*, dan *phishing PDF*. Berikut ini bentuk dan makna motif bahasa dalam aksi kejahatan *phishing*.

3.1 *Deceptive Phishing*

Deceptive phishing adalah salah satu bentuk serangan siber yang dilakukan melalui pesan teks yang dirancang secara manipulatif, dengan menyamar sebagai entitas yang kredibel seperti bank, lembaga pemerintah, atau layanan digital populer. Tujuan utama dari modus ini adalah untuk mengelabui korban agar menyerahkan informasi pribadi seperti data login, nomor kartu kredit, atau identitas diri. Pelaku memanfaatkan teknik *social engineering* dengan meniru gaya bahasa formal lembaga resmi, memanfaatkan citra institusi terpercaya, serta membangun rasa urgensi atau ancaman agar korban cepat merespons. Bahasa yang digunakan sering kali mengandung perintah implisit maupun eksplisit.

Dalam penelitian ini, *deceptive phishing* dianalisis melalui pendekatan analisis wacana dan linguistik forensik secara sistematis, berdasarkan tahapan analisis data dari (Miles & Huberman, 1994). Pada tahap display *data*, dikumpulkan sejumlah pesan *phishing* sebagai objek kajian. Selanjutnya, pada tahap identifikasi, dianalisis struktur kalimat, penggunaan diksi otoritatif, serta gaya komunikasi yang meniru institusi resmi. Tahap klasifikasi kemudian memetakan strategi linguistik seperti penggunaan urgensi palsu, peniruan otoritas, dan bahasa persuasif. Terakhir, tahap makna dan tujuan menafsirkan maksud tersembunyi dari pesan tersebut, yang secara pragmatis berfungsi sebagai tindakan ujaran manipulatif *(manipulative speech act*) untuk mengarahkan perilaku korban ke arah yang merugikan, seperti membocorkan informasi sensitif atau mengakses tautan berbahaya.

3.1.1 Informasi yang Mengatasnamakan Facebook (Data 01)

Salah satu modus *phishing* yang paling sering ditemukan adalah penggunaan nama merek terkenal seperti Facebook untuk menciptakan kesan otoritatif. Dalam kasus ini (Data 01), pelaku mengirimkan pesan yang berisi ancaman penonaktifan akun jika korban tidak segera melakukan verifikasi. Pesan tersebut menampilkan elemen bahasa persuasif yang memanfaatkan *coercive language* atau bahasa paksaan, dengan tujuan menekan psikologis korban agar segera mengambil tindakan (Boux dkk., 2023). Struktur pesan biasanya berisi perintah langsung seperti "Harap verifikasi akun Anda segera untuk menghindari pemblokiran." Meskipun sekilas terlihat resmi, dalam analisis linguistik ditemukan indikasi ketidakaslian, seperti kesalahan penulisan nama Facebook ("fecebook" alih-alih "Facebook"), yang menunjukkan bahwa pesan tersebut berasal dari sumber yang tidak valid. Strategi ini juga mengandalkan *speech act* perintah, yang bertujuan untuk menciptakan ilusi urgensi sehingga korban bertindak impulsif tanpa memeriksa kebenaran pesan.

3.1.2 Pesan yang Mengatasnamakan Instagram (Data 02)

Selain ancaman, *deceptive phishing* juga sering menggunakan strategi berbasis insentif, (Data 02), yakni ketika korban dijanjikan sesuatu yang berharga sebagai imbalan mengikuti instruksi dalam pesan. Salah satu modus yang dianalisis adalah *phishing* yang mengatasnamakan Instagram dan menjanjikan lencana biru (*verified badge*) kepada korban. Pesan ini merupakan contoh *reward-based phishing*, di mana korban dimanipulasi dengan harapan memperoleh keuntungan tertentu (Tomicic, 2023). Pelaku meniru struktur komunikasi resmi Instagram, meskipun domain pengirim tidak berasal dari alamat resmi. Dari sudut pandang analisis wacana, pesan ini dirancang dengan struktur persuasi yang bertujuan untuk mengelabui korban agar mengikuti arahan tanpa mempertanyakan keasliannya. Kalimat seperti *"Akun Anda akan menerima lencana biru jika segera mengisi formulir ini"* digunakan untuk membangun ekspektasi positif dan meningkatkan kemungkinan korban terjebak dalam penipuan.

3.1.3 Informasi yang Menyamar Sebagai Lembaga Pemerintahan (Data 03)

Phishing juga sering dilakukan dengan menyamar sebagai lembaga pemerintahan, yang bertujuan untuk meningkatkan kredibilitas pesan. Dalam salah satu kasus pada Data 03, pelaku mengklaim bahwa pemilik E-KTP berhak menerima kompensasi tertentu, sehingga mendorong korban untuk segera mengikuti instruksi yang diberikan. Pesan ini memanfaatkan *pseudo-legitimacy*, yaitu strategi yang menggunakan bahasa formal untuk menciptakan ilusi keabsahan (Benavides-Astudillo dkk., 2023). Selain itu, pesan juga menggunakan elemen urgensi, seperti penyebutan tanggal tertentu, yang bertujuan untuk membuat korban merasa harus segera bertindak agar tidak kehilangan kesempatan. Secara linguistik, pesan ini termasuk dalam kategori *fraudulent discourse*, yang penggunaan istilah administratif bertujuan untuk meningkatkan kepercayaan terhadap informasi palsu. Teknik ini juga mengandung *coercive language*, yang secara psikologis menekan korban untuk bertindak tanpa melakukan verifikasi lebih lanjut.

3.1.4 Pesan yang Mengatasnamakan Pihak JNE (Data 04)

Selain menyamar sebagai lembaga pemerintahan, *phishing* juga sering kali dilakukan dengan menggunakan nama perusahaan logistik seperti JNE. Dalam Data 04, pelaku menjanjikan Samsung S7 sebagai hadiah, dengan syarat korban membayar biaya administrasi sebesar Rp100.000 dalam bentuk pulsa. Modus ini merupakan contoh dari *low-cost, high-reward trap*, yaitu strategi yang membujuk korban dengan tawaran hadiah bernilai tinggi tetapi dengan biaya kecil yang harus dikeluarkan (Christiansen, 2021). Pesan ini juga menggunakan *scam linguistics*, seperti *"Rezeki Tidak Kemana"* digunakan untuk membangun kesan bahwa korban sedang mendapatkan kesempatan emas yang harus segera diambil. Dalam analisis wacana, pola ini dirancang untuk mengurangi

kewaspadaan korban, sehingga mereka lebih mudah terpengaruh dan tidak mempertanyakan validitas pesan sebelum mengambil tindakan.

3.1.5 Pesan Mengatasnamakan Artis Terkenal (Data 05)

Salah satu teknik *deceptive phishing* yang semakin populer adalah penggunaan nama figur publik untuk meningkatkan kredibilitas pesan. Dalam Data 05, pelaku menyamar sebagai Baim Wong dan mengadakan *giveaway* palsu dengan syarat korban mengetik huruf *"p"* sebanyak-banyaknya di kolom komentar. Strategi ini termasuk dalam *celebrity endorsement deception*, di mana pelaku berpura-pura menjadi tokoh terkenal agar pesan phishing terlihat lebih meyakinkan (Salloum dkk., 2023). Teknik yang digunakan adalah *perceptual mimicry*, yang menggunakan akun palsu dengan nama yang mirip dengan selebritas asli, misalnya *"BaIm Mong"* yang sekilas menyerupai *"Baim Wong"*. Pesan ini juga mengandalkan *herd mentality,* yaitu strategi yang memanfaatkan psikologi sosial di mana orang cenderung mengikuti tren yang sedang populer. Dalam analisis wacana, modus ini dikenal sebagai *mass engagement trap,* di mana keterlibatan massal digunakan untuk meningkatkan kredibilitas penipuan dan meyakinkan lebih banyak korban agar ikut serta.

3.1.6 Pesan Peringatan Mengatasnamakan Facebook (Data 06)

Selain strategi insentif dan penyamaran sebagai figur publik, *deceptive phishing* juga sering mengeksploitasi rasa takut korban. Dalam Data 06, pelaku mengatasnamakan Facebook dan mengklaim bahwa akun korban akan segera diblokir jika tidak melakukan verifikasi. Pesan ini termasuk dalam *threat-based phishing*, di mana ancaman digunakan sebagai alat utama untuk memaksa korban bertindak impulsif (Gil, 2018). Teknik yang digunakan dalam pesan ini adalah *fear appeal*, yaitu strategi persuasi yang mengeksploitasi ketakutan agar korban segera mengikuti instruksi tanpa memeriksa keabsahan informasi. Dalam linguistik forensik, pola ini masuk dalam kategori *coercive speech act*, yaitu tindakan tutur yang bersifat memaksa agar korban segera memberikan informasi pribadi atau kredensial akun mereka. Selain itu, *phishing* ini sering menggunakan domain palsu, seperti *weebly.com*, yang menyerupai domain asli tetapi sebenarnya tidak terkait dengan Facebook.

3.1.7 Informasi Mengatasnamakan Tokopedia (Data 07)

Pesan yang mengumumkan hadiah penanak nasi dari Tokopedia (Data 07) adalah contoh *phishing* yang dirancang untuk mencuri informasi pribadi korban. Dalam pesan ini, pelaku menggunakan bahasa yang menarik perhatian dengan menawarkan hadiah menarik, seperti klaim hadiah "*penanak nasi senilai Rp 1.000.000"* yang dikirimkan secara gratis. Penyusunan kata yang sederhana namun menggugah ini bertujuan untuk memikat penerima pesan dan mendorong mereka untuk segera bertindak tanpa berpikir panjang. Pesan ini berusaha menciptakan rasa antusiasme dan ketergantungan pada iming-iming hadiah, sebuah teknik umum dalam *phishing* yang memanfaatkan aspek psikologis korban untuk mengabaikan kewaspadaan mereka terhadap potensi penipuan. Dengan menggunakan platform pesan pribadi yang dikenal, seperti WhatsApp, pelaku memanfaatkan kedekatan dan kepercayaan korban terhadap aplikasi tersebut untuk meningkatkan keberhasilan penipuan. Teknik ini juga memanfaatkan konsep *coercive language* di mana pelaku menciptakan rasa urgensi yang memaksa korban untuk bertindak cepat tanpa verifikasi lebih lanjut (Boux dkk., 2023).

3.1.8 Email Mengatasnamakan POS Indonesia (Data 08)

Email yang mengatasnamakan PT Pos Indonesia (Data 08) adalah contoh *phishing* yang bertujuan untuk mencuri informasi pribadi penerima email. Pesan ini menggunakan bahasa formal dan profesional yang sering digunakan dalam komunikasi bisnis resmi, seperti frasa *"kegagalan pengiriman barang"* dan *"belum membayar bea masuk"*, yang dirancang untuk menimbulkan rasa urgensi dan otoritas, mendorong penerima untuk segera bertindak tanpa berpikir panjang. Pelaku

phishing memanfaatkan kepercayaan umum terhadap lembaga resmi seperti PT Pos Indonesia, dengan menggunakan logo dan format yang menyerupai email resmi dari organisasi tersebut. Teknik *social engineering* ini bertujuan menciptakan ilusi keabsahan pesan agar penerima tidak ragu-ragu untuk mengikuti instruksi yang diberikan. Tautan yang ada dalam email ini mengarah ke situs web yang tidak sah, berpotensi mengumpulkan informasi pribadi atau menginfeksi perangkat korban dengan malware. Dalam analisis wacana, ini merupakan contoh dari *pseudo-legitimacy*, di mana pelaku mencoba menciptakan kesan keabsahan melalui penggunaan elemen-elemen visual yang menyerupai komunikasi resmi (Benavides-Astudillo dkk., 2023).

3.1.9 Pesan Mengatasnamakan TikTok (Data 09)

Pesan yang menawarkan *"pendapatan stabil minimal 300.000 IDR per hari"* dengan menggunakan nama TikTok (Data 09) adalah contoh *phishing* yang memanfaatkan harapan korban untuk mendapatkan keuntungan ekonomi dengan cara mudah. Pesan ini menarik perhatian dengan menawarkan kesempatan untuk menghasilkan uang secara cepat, sebuah klaim yang sangat menggoda bagi banyak orang. Selain itu, penggunaan tautan yang mencurigakan seperti *"https://watiktok.com/id1"* merupakan indikasi utama dari *phishing*. Tautan ini tidak berasal dari domain resmi TikTok dan dirancang untuk menipu korban agar mengkliknya. Dalam penelitian Balamurugan & Jayabharathy (2022), penggunaan tautan yang disamarkan adalah taktik umum yang digunakan dalam *phishing* untuk mengelabui korban agar memberikan data pribadi atau mengakses situs web yang berbahaya. Pesan ini memanfaatkan taktik *social engineering* dan juga menggugah emosi korban dengan menjanjikan kesempatan besar yang seolah tidak boleh dilewatkan, sehingga korban terjebak tanpa berpikir kritis. Teknik ini sering kali dikenal dengan *reward-based phishing*, yakni memanipulasi korban dengan janji hadiah atau keuntungan yang menggiurkan (Tomicic, 2023).

3.1.10 Pesan Mengatasnamakan BRI (Data 10)

Pesan yang mengatasnamakan bank BRI (Data 10) bertujuan untuk menipu korban agar mengungkapkan informasi pribadi atau mengakses situs web yang berbahaya. Pesan ini menggunakan bahasa yang tampak resmi dengan menyebutkan *"Nasabah bank BRI yang terhormat"*, untuk menciptakan kesan otoritas dan kredibilitas, yang seharusnya membuat penerima merasa bahwa pesan tersebut sah. Namun, pesan ini mengandung sejumlah kesalahan tata bahasa yang jelas, seperti *"komfirmasi"* dan *"Terimakasi"*, yang dapat mengindikasikan bahwa pesan tersebut tidak berasal dari sumber resmi. Penyerang dalam *phishing* ini juga menggunakan tautan yang mencurigakan seperti *"http:/perubahantarifbri6500"*, yang bukan merupakan URL resmi dari bank BRI. Tautan ini adalah indikator utama bahwa pesan tersebut adalah penipuan. Pesan ini mencoba memanipulasi korban dengan urgensi dan klaim untuk mengisi formulir atau mengklik tautan tanpa memverifikasi keaslian pesan tersebut. Keberadaan kesalahan bahasa dan URL yang tidak sah menunjukkan bahwa pelaku tidak memperhatikan detail atau memiliki kemampuan bahasa yang kurang, yang semakin memperkuat kecurigaan bahwa pesan ini adalah phishing. *Speech act* dalam hal ini mengacu pada tindakan bahasa yang memiliki akibat langsung berupa pencurian data pribadi korban (Gil, 2018).

3.2 Phishing APK

Phishing APK merupakan salah satu bentuk kejahatan siber yang mengandalkan distribusi aplikasi berbahaya berbasis Android (APK) untuk menipu pengguna. Modus ini umumnya menyamar sebagai entitas yang tampak kredibel atau memanfaatkan situasi yang bersifat mendesak, seperti undangan pernikahan, surat tilang, atau pemberitahuan pengiriman paket, guna memancing perhatian dan respons dari korban. Teknik ini bekerja dengan memanipulasi psikologi target melalui strategi *social engineering*, yaitu memanfaatkan emosi seperti rasa ingin tahu, ketakutan, atau kepercayaan

terhadap institusi, agar korban bersedia mengunduh dan memasang aplikasi APK yang sebenarnya mengandung *malware* atau skrip jahat lainnya.

Dalam ranah linguistik forensik, analisis terhadap pesan-pesan *phishing* ini dilakukan secara sistematis dengan merujuk pada tahapan analisis data dari (Miles & Huberman, 1994). Pertama, tahap *display* data bertujuan untuk menyajikan pesan-pesan *phishing* yang menjadi objek kajian. Kedua, dilakukan identifikasi untuk mengurai karakteristik linguistik dalam pesan, seperti pilihan kata, gaya bahasa, dan struktur kalimat. Ketiga, dilakukan klasifikasi terhadap elemen-elemen bahasa tersebut ke dalam kategori strategi manipulatif yang digunakan oleh pelaku. Terakhir, tahap makna dan tujuan berfokus pada penafsiran maksud tersembunyi di balik pesan tersebut serta potensi ancaman yang ditimbulkannya terhadap korban. Pendekatan ini memungkinkan analisis yang menyeluruh dan berbasis teori dalam mengungkap praktik kejahatan digital melalui bahasa.

3.2.1 Undangan APK (Data 11)

Modus *phishing* dengan menggunakan undangan pernikahan digital merupakan strategi manipulatif yang mengeksploitasi norma sosial masyarakat. Pada Data 11 penggunaan judul *file "Surat Undangan Pernikahan Digital"* menjadi umpan yang efektif karena pernikahan adalah peristiwa penting yang secara kultural mengundang perhatian. Dalam pesan ini, pelaku menggunakan ungkapan *"Kami harap kehadirannya"* yang secara pragmatis menunjukkan kesan kedekatan dan urgensi. Hal ini merupakan bentuk penggunaan strategi kesopanan yang diselipkan untuk membangun kredibilitas pesan, sesuai dengan temuan Pritzker (2020) bahwa bahasa dalam konteks digital dapat membentuk dan mengarahkan emosi serta respons pembaca.

Dalam perspektif linguistik forensik, pesan ini diklasifikasikan sebagai *clickbait phishing*, di mana bahasa bersifat ambigu namun membangkitkan rasa ingin tahu. Strategi ini didukung oleh penggunaan frasa yang tidak menjelaskan secara rinci identitas pengirim atau detail acara, melainkan mendorong korban untuk membuka file APK demi mendapatkan informasi lebih lanjut. Tindakan tersebut membuka peluang infeksi *malware* yang tertanam dalam APK. Oleh karena itu, modus ini menunjukkan bagaimana teknik linguistik seperti kesopanan, ambiguitas, dan ekspektasi sosial digunakan untuk mengecoh korban dan menciptakan tindakan impulsif.

3.2.2 Resi J&T APK (Data 12)

Pesan *phishing* yang mengklaim adanya pengiriman paket dari J&T pada Data 12 menggunakan pendekatan persuasif melalui bahasa sopan dan informal, seperti *"Assalamualaikum kak, selamat siang kak"*. Ini mencerminkan strategi kedekatan sosial yang bertujuan membangun rasa percaya dan kenyamanan antara pengirim dan penerima. Frasa selanjutnya, *"Cek Resi Paket JNT (apk)"*, adalah instruksi eksplisit yang mendorong tindakan langsung. Dalam analisis pragmatik, pola ini menggambarkan manipulasi melalui kesopanan semu yang berpotensi mengalihkan perhatian korban dari elemen mencurigakan seperti ekstensi file APK.

Secara linguistik forensik, modus ini termasuk dalam *service impersonation phishing*, di mana pelaku menyamar sebagai entitas terpercaya seperti layanan ekspedisi. Strategi ini memanfaatkan urgensi dan kebutuhan korban khususnya mereka yang tengah menunggu paket untuk memanipulasi respons cepat tanpa proses verifikasi. Struktur pesan yang menggabungkan empati palsu dan perintah teknis menunjukkan bahwa pelaku memahami cara kerja psikologi linguistik dalam komunikasi daring. Hal ini menjadi perhatian penting dalam investigasi wacana kriminal digital karena pelaku menggunakan elemen bahasa untuk mengaburkan niat jahat di balik komunikasi yang tampak ramah.

3.2.3 Surat Tilang APK (Data 13)

Pesan *phishing* pada (Data 13) ini menyatakan bahwa penerima telah melakukan pelanggaran lalu lintas, dengan instruksi untuk membuka file *"Surat Tilang-1.0.apk"*. Penggunaan bahasa resmi dan struktur kalimat seperti *"Kami dari kepolisian menginformasikan bahwa bapak/ibu melakukan pelanggaran"* berfungsi menciptakan citra otoritatif. Dalam pendekatan wacana forensik, ini disebut sebagai strategi *pseudo-authority*, yaitu klaim kekuasaan atau legitimasi yang tidak sah untuk mengarahkan perilaku korban (Andriyanto, 2022). Bahasa formal yang digunakan dalam konteks ancaman hukum meningkatkan tekanan psikologis dan mempercepat reaksi korban tanpa analisis kritis.

Dari sudut linguistik, pesan ini memadukan tiga teknik utama: klaim otoritas palsu, eksploitasi rasa takut, dan instruksi langsung. Frasa seperti *"Silakan buka aplikasi"* memberikan perintah eksplisit yang menambah kesan mendesak. Modus seperti ini masuk dalam kategori *fear-based phishing***,** yakni strategi yang mengandalkan ketakutan sebagai alat manipulasi (Gil, 2018). Dengan memanfaatkan ketakutan korban terhadap ancaman hukum, pelaku berhasil menurunkan kewaspadaan dan memanipulasi tindakan korban. Pesan semacam ini memperlihatkan bagaimana kekuatan bahasa dapat digunakan secara strategis dalam kejahatan digital untuk menghasilkan kepatuhan melalui tekanan emosional.

3.2.4 Foto Paket J&T APK (Data 14)

Pelaku *phishing* pada (Data 14) mengirimkan pesan yang menyebutkan adanya paket dengan nama penerima dan menyertakan file APK untuk melihat foto paket. Kalimat seperti *"Ada Paket di J&T Express Nama SALMAH (LIHAT Foto Paket APK)"* mengandung elemen manipulatif yang dirancang untuk membangkitkan rasa penasaran korban. Namun, adanya kesalahan penulisan seperti *"Expeess"* dan nama yang salah ketik *"SALNAH"* menjadi indikator linguistik bahwa pesan ini mencurigakan. Dalam analisis linguistik forensik, kesalahan ejaan dan tata bahasa sering ditemukan dalam *phishing* karena tidak adanya standar profesional dalam penyusunan pesan (Santoso, 2023).

Strategi yang digunakan dalam pesan ini mencakup pemalsuan identitas layanan resmi, eksploitasi rasa ingin tahu, dan pemanfaatan informasi ambigu. Frasa yang tidak memberikan detail lengkap tentang paket mendorong korban untuk mencari tahu lebih lanjut dengan membuka file yang disisipkan. Hal ini merupakan bentuk *curiosity-based phishing*, di mana pelaku mengandalkan rasa penasaran untuk menghasilkan klik. Dalam konteks ini, wacana digunakan sebagai alat penyamaran niat jahat, dan kesalahan bahasa justru menjadi petunjuk penting bagi analisis forensik untuk mengungkap keaslian pesan. Maka, pesan ini menunjukkan bagaimana ketidaksempurnaan linguistik dapat menjadi kunci penting dalam investigasi digital.

3.3 *Smishing*

Smishing merupakan salah satu bentuk kejahatan siber yang memanfaatkan pesan singkat (SMS) atau aplikasi pesan instan seperti WhatsApp sebagai media utama untuk menipu korban. Modus ini bekerja dengan mengirimkan pesan teks yang tampak resmi atau mendesak, seperti pemberitahuan bank, konfirmasi pengiriman, atau tawaran hadiah. Pesan biasanya disertai tautan atau nomor kontak yang diarahkan ke situs palsu atau aplikasi berbahaya. Pelaku *smishing* mengeksploitasi kepercayaan korban terhadap institusi serta memanipulasi emosi seperti ketakutan, rasa ingin tahu, atau keinginan untuk mendapatkan keuntungan ekonomi. Strategi ini tergolong dalam praktik rekayasa sosial (*social engineering*), yang berusaha mempengaruhi perilaku korban melalui pesan-pesan yang tampak wajar di permukaan, namun sarat dengan niat tersembunyi.

Dalam lingkup linguistik forensik, *smishing* dianalisis melalui pendekatan sistematis seperti yang dikemukakan oleh (Miles & Huberman, 1994), yang mencakup empat tahapan utama. Pertama, pada tahap display data, dikumpulkan pesan-pesan *smishing* sebagai data utama untuk dianalisis. Kedua,

dilakukan identifikasi terhadap unsur kebahasaan dalam pesan, seperti pemilihan diksi, penggunaan gaya formal, struktur kalimat perintah, serta adanya penanda otoritas semu. Ketiga, unsur-unsur tersebut kemudian diklasifikasikan ke dalam strategi manipulatif seperti *pseudo-authority*, urgensi palsu, dan daya tarik ekonomi. Terakhir, tahap makna dan tujuan menyoroti fungsi pragmatik pesan sebagai tindakan ujaran (*speech act*) yang secara tidak langsung mengarahkan korban untuk membocorkan informasi pribadi atau mengambil tindakan berisiko. Analisis ini membantu mengungkap pola penipuan berbasis bahasa serta kontribusinya terhadap pencegahan kejahatan digital.

3.3.1 Informasi Kartu Prakerja (Data 15)

Data (15) menunjukkan pesan berantai yang menawarkan akses pendaftaran Kartu Prakerja melalui situs web yang mencurigakan. Pesan ini menggunakan format bahasa formal dan profesional, meniru gaya komunikasi resmi pemerintah. Frasa seperti "pendaftaran Kartu Prakerja" dan "data pribadi" memperkuat kesan legitimasi. Analisis linguistik menunjukkan bahwa pilihan leksikal dan struktur kalimat dirancang untuk membangun kredibilitas, seolah-olah pesan tersebut berasal dari lembaga resmi (Akande dkk., 2023). Secara strategi, pesan ini mengandung teknik eksploitasi otoritas dan rasa urgensi. Pelaku menggunakan kedok program bantuan pemerintah yang familiar bagi masyarakat, dengan tujuan mengeksploitasi kepercayaan sosial terhadap institusi negara. Tindakan linguistik dalam pesan ini tergolong speech act yang manipulatif, yaitu menyuruh penerima segera mengakses tautan dan memasukkan data pribadi. Ini mencerminkan tindakan *illocutionary force* yang memiliki konsekuensi langsung terhadap keamanan digital korban (Lestari & Hartati, 2020).

3.3.2 Pesan Berantai WHO Palsu (Data 16)

Data 16 memperlihatkan pesan berantai di WhatsApp yang mengklaim adanya paket internet gratis dari WHO dan WhatsApp. Bahasa dalam pesan menggunakan gaya promosi dengan frasa menggoda seperti *"paket internet gratis sebesar 50GB".* Diksi yang digunakan membentuk efek sugestif dan memicu tindakan impulsif. Menurut Wallis (2022), kekuatan bahasa dalam konteks digital terletak pada kemampuannya menyamarkan realitas dan membangun kepercayaan palsu. Pesan ini menggabungkan strategi eksploitasi rasa ingin tahu, manipulasi urgensi, dan penyamaran sebagai entitas resmi. Teknik *social engineering* diaktifkan melalui pencantuman klaim hadiah dan tautan mirip tautan resmi. Tujuan pragmatis dari pesan ini adalah untuk mendorong korban mengeklik tautan dan memasukkan data pribadi. Dalam konteks linguistik forensik, tindakan komunikasi semacam ini merupakan bagian dari *indirect speech act* dengan dampak langsung pada perilaku korban.

3.3.3 Pesan Kode Verifikasi WhatsApp (Data 17)

Data 17 mencakup pesan yang mengatasnamakan WhatsApp, mengklaim adanya afiliasi resmi. Bahasa yang digunakan cenderung formal namun diselingi dengan ancaman atau janji hadiah. Pilihan kata seperti *"verifikasi akun"* dan *"penangguhan"* digunakan untuk menciptakan kesan urgensi dan otoritas palsu, ciri khas dari *pseudo-authority* dalam linguistik forensik (Andriyanto, 2022). Pesan ini mengandung strategi manipulasi berbasis rasa takut dan teknik penyamaran institusional. Dengan menggabungkan elemen visual seperti logo dan bahasa otoritatif, pelaku berupaya mengelabui korban agar memberikan kode verifikasi atau data pribadi lainnya. Pragmatik pesan ini jelas menunjukkan niat manipulatif melalui *speech act* yang seolah bersifat informatif, padahal menyasar pencurian data. Tujuan akhirnya adalah akses ke akun pribadi korban, terutama akun WhatsApp.

3.3.4 Pesan Berantai Iming-Iming Hadiah Uang (Data 18)

Data 18 menunjukkan pesan *phishing* yang menawarkan hadiah uang dari *brand* kecantikan Kedas Beauty. Pesan ini menyatakan bahwa penerima memenangkan *giveaway* dan harus mengakses

tautan tertentu. Bahasa yang digunakan bersifat sugestif dan memanfaatkan harapan ekonomi korban. Frasa seperti *"giveaway jutaan rupiah"* dan *"klaim sekarang"* menunjukkan intensi persuasif yang tinggi (Gallo dkk., 2024). Strategi utama yang digunakan adalah eksploitasi kepercayaan terhadap *brand* dan iming-iming hadiah. Teknik *clickbait phishing* dipadukan dengan daya tarik ekonomi untuk menurunkan pertahanan kognitif korban. Dalam kajian linguistik forensik, tindakan dalam pesan ini tergolong sebagai *speech act* perintah terselubung, dengan daya manipulatif tinggi terhadap perilaku penerima. Tujuannya adalah agar korban memberikan data pribadi atau bahkan uang sebagai *"biaya administrasi"*.

3.3.5 Pesan Berantai Bantuan BPJS (Data 19)

Data (19) menampilkan pesan dengan karakteristik unik berupa penggunaan angka dan huruf campuran seperti *"D4n4 B4ntu4n D4ri Kanotr Pusat".* Bahasa yang digunakan bersifat ambigu, dan tautan bit.ly disematkan dalam pesan untuk menyembunyikan alamat asli situs *phishing*. Teknik ini dimaksudkan untuk menghindari deteksi otomatis oleh filter spam serta membangkitkan rasa penasaran penerima. Pesan ini menggunakan strategi linguistik manipulatif berupa pengacakan karakter (*leetspeak*), eksploitasi bantuan sosial, dan penyamaran melalui tautan pendek. *Speech act* dalam pesan ini bersifat ilokusiif dengan efek langsung pada tindakan penerima, yaitu mengklik tautan. Tujuan pragmatisnya adalah mengarahkan korban ke situs berbahaya yang dapat mencuri data pribadi atau menanamkan *malware*, yang merupakan ciri khas *phishing* berbasis tautan.

3.3.6 Pesan Permohonan Mengisi Kuesioner UNICEF Palsu (Data 20)

Data 20 menunjukkan pesan berantai yang mengklaim bahwa UNICEF Indonesia memberikan uang tunai setelah mengisi kuesioner. Pesan ini menyertakan angka pasti *"Rp. 11.024.000"* untuk menciptakan kesan konkret dan meyakinkan. Bahasa yang digunakan formal dan terstruktur, serta mencantumkan unsur organisasi internasional yang memiliki kredibilitas tinggi, seperti UNICEF. Pesan ini menggunakan strategi penyamaran lembaga terpercaya, janji hadiah ekonomi, dan taktik desakan sosial. Teknik *social engineering* digunakan untuk membuat korban percaya bahwa mereka hanya perlu mengisi survei untuk menerima uang. *Speech act* dalam pesan ini berfungsi mengarahkan tindakan korban untuk membocorkan data pribadi secara sukarela. Tujuannya adalah memperoleh data demografis yang bisa dijual atau digunakan untuk kejahatan siber lainnya.

3.3.7 Pesan Berantai Tawaran Pinjaman Online (Data 21)

Data 21 menampilkan pesan SMS yang mengklaim pinjaman sebesar Rp 20.000.000 telah disetujui dan meminta penerima mengklik tautan untuk konfirmasi. Bahasa yang digunakan sangat persuasif dan memberikan kesan resmi. Namun, terdapat kesalahan ejaan seperti *"disetujul"* dan *"mengonfimasi"* serta tautan mencurigakan *"idnsloans.com"* yang bukan domain terpercaya. Strategi yang digunakan dalam pesan ini mencakup eksploitasi kebutuhan ekonomi, penyamaran otoritas finansial, dan penggunaan urgensi palsu. Analisis linguistik menunjukkan bahwa pesan ini dimaksudkan untuk mendorong korban melakukan tindakan tanpa berpikir panjang. Tindakan bahasa (*speech act*) dalam bentuk perintah untuk mengklik tautan menjadi alat utama manipulasi. Tujuannya adalah mencuri data finansial atau mengarahkan korban ke situs *malware*.

5 Simpulan

Berdasarkan kajian yang telah dilakukan, ditemukan 21 temuan yang mengandung pesan dan informasi berisi aksi *phishing*. Setiap data mengandung makna yang kompleks, dengan penggunaan bahasa yang manipulatif dan persuasif untuk mempengaruhi korban agar mengikuti perintah pelaku. Bahasa persuasif dan manipulatif ini dirancang secara cermat untuk menciptakan ilusi kepercayaan dan urgensi, yang membuat korban cenderung memberikan informasi pribadi tanpa berpikir panjang. Hal ini menunjukkan bahwa penggunaan strategi komunikasi dalam *phishing* sangat terencana dan

berfokus pada pemanfaatan kelemahan psikologis manusia. Kesimpulannya, bahasa dalam aksi kejahatan *phishing* bukan sekadar alat komunikasi, melainkan senjata yang digunakan untuk memanipulasi korban. Strategi linguistik yang digunakan dalam pesan *phishing* menunjukkan bahwa pelaku memahami cara memanipulasi persepsi dan tindakan korban melalui penggunaan kata-kata yang tepat. Penelitian ini menegaskan pentingnya literasi digital dan kesadaran akan taktik manipulatif yang digunakan dalam kejahatan siber. Pemahaman bahasa yang digunakan dalam konteks *phishing*, membuat individu dapat lebih waspada dan mampu melindungi diri dari ancaman semacam ini.

Disclosure Statement

The author(s) claim there is no conflict of interest.

Referensi

AAG IT Support. (2024). The latest phishing statistics (updated June 2024). *AAG IT Support*. https://www.aagit.com

Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O. & Fatokun, A. (2023). Smsprotect: An automatic smishing detection mobile application. *ICT Express*, *9*(2), 168–176. https://doi.org/10.1016/j.icte.2022.05.009

Amro, B. (2018). Phishing techniques in mobile devices. *Journal of Computer and Communications*, *06*(02), 27–35. https://doi.org/10.4236/jcc.2018.62003

Andriyanto, T. (2022). Komunikasi termediasi penipuan dengan modus business email compromise. *Jurnal Riset Komunikasi*, *5*(2), 220–243. https://doi.org/10.38194/jurkom.v5i2.627

Anggana, N. D. (2024, 31. Mei). *Phishing: Berkenalan dengan si ahli penipuan*. https://widyasecurity.com/2024/05/31/phishing-berkenalan-dengan-si-ahli-penipuan/

Balamurugan, G. & Jayabharathy, J. (2022). Cyberbully classification based on tweet texts for detection of phishing links. Dalam R. Asokan, D. P. Ruiz, Z. A. Baig & S. Piramuthu (Ed.), *Smart Data Intelligence* (hlm. 367–374). Springer Nature. https://doi.org/10.1007/978-981-19-3311-0_31

Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Nuñez-Agurto, D. & Rodríguez-Galán, G. (2023). A phishing-attack-detection model using natural language processing and deep learning. *Applied Sciences (Switzerland)*, *13*(9), 5275. https://doi.org/10.3390/app13095275

Boux, I. P., Margiotoudi, K., Dreyer, F. R., Tomasello, R. & Pulvermüller, F. (2023). Cognitive features of indirect speech acts. *Language, Cognition and Neuroscience*, *38*(1), 40–64.

Caniago, K. & Sutabri, T. (2023). Tindak kejahatan phising di sektor pelayan di Universitas Bina Insan Lubuklinggau. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, *8*(1), 117–125. https://doi.org/10.30645/jurasik.v8i1.548

Christiansen, T. W. (2021). Linguistics and Deception Detection (DD): A work in progress. *Studies in Logic, Grammar and Rhetoric*, *66*(2), undefined-undefined. https://doi.org/10.2478/slgr-2021-0011

Dharani, L. I. C., Idayanti, S. & Rahayu, K. (2024). *Perlindungan hukum terhadap tindakan phishing di media sosial*. Penerbit NEM.

Fitriarti, E. A. (2019). Urgensi literasi digital dalam menangkal hoax informasi kesehatan di era digital. *Metacommunication; Journal of Communication Studies*, *4*(2), 234–246. https://doi.org/10.20527/mc.v4i2.6929

Gallo, L., Gentile, D., Ruggiero, S., Botta, A. & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671. https://doi.org/10.1016/j.cose.2023.103671

Gil, P. (2018). What Is "Whaling?" *Lifewire*. https://www.mendeley.com/catalogue/c1063411-5a1a-3135-b7d0-189bb59bc1b3/

Grecya, E., Sinurat, B., Yahya, I. E., Ginting, N. A., Tambunan, M. Y. K. T., Ahmid, I. A. & Ivanna, J. (2021). Kontribusi mahasiswa sebagai aktor pendidikan dalam menghadapi rendahnya literasi terhadap berita hoax: Aktor atau penonton. *Jotika Journal in Education*, *1*(1), 10–17. https://doi.org/10.56445/jje.v1i1.14

Karamagi, R. & Ally, S. (2023). Security risk scale: A case of email phishing detection using text mining. *Journal of ICT Systems*, *1*(2), 93–108. https://doi.org/10.56279/jicts.v1i2.43

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F. & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480–501. https://doi.org/10.1177/10439862211027986

Kothamasu, G. A., Venkata, S. K. A., Pemmasani, Y. & Mathi, S. (2023). An Investigation on vulnerability analysis of phishing attacks and countermeasures. *International Journal of Safety and Security Engineering*, *13*(2), 333–340. https://doi.org/10.18280/ijsse.130215

Lestari, T. & Hartati, E. (2020). A pragmatics analysis of speech act in Thor movie. *ELTICS : Journal of English Language Teaching and English Linguistics*, *4*(2), undefined-undefined. https://doi.org/10.31316/eltics.v4i2.524

Lin, Y., Liu, R., Divakaran, D. M., Ng, J. Y., Chan, Q. Z., Lu, Y., Si, Y., Zhang, F. & Dong, J. S. (2021). Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. *Proceedings of the 30th USENIX Security Symposium*, 3793–3810.

Lokapala, Y. H., Nurfauzi, F. J. & Wdowaty, Y. (2024). Aspek yuridis kejahatan phishing dalam ketentuan hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *5*(1), 19–24. https://doi.org/10.18196/ijclc.v5i1.19853

Lwin Tun, Z. & Birks, D. (2023). Supporting crime script analyses of scams with natural language processing. *Crime Science*, *12*(1), 1. https://doi.org/10.1186/s40163-022-00177-w

Miles, M. B. & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook - Matthew B. Miles, A. Michael Huberman - Google Buku. *Sage Publications*.

Muftiadi, A., Agustina, T. P. M. & Evi, M. (2022). Studi kasus keamanan jaringan komputer: Analisis Ancaman phising terhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik*, *1*(2), 60–65. https://doi.org/10.55904/hexatech.v1i2.346

Napitupulu, D. (2017). Kajian peran cyber law dalam memperkuat keamanan sistem informasi nasional. *Deviance Jurnal Kriminologi*, *1*(1), 100–113. https://doi.org/10.36080/djk.595

Nugroho, H., Ihsan, M. N., Haryoko, A., Ma`arif, F. & Alifah, F. (2023). Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phising. *Alahyan Jurnal*

Pengabdian Masyarakat Multidisiplin, *1*(2), 104–111. https://doi.org/10.61492/ecos-preneurs.v1i2.60

Orunsolu, A. A., Sodiya, A. S. & Akinwale, A. T. (2022). A predictive model for phishing detection. *Journal of King Saud University - Computer and Information Sciences*, *34*(2), 232–247. https://doi.org/10.1016/j.jksuci.2019.12.005

Pritzker, S. E. (2020). Language, emotion, and the politics of vulnerability. *Annual Review of Anthropology*, *49*, 241–256. https://doi.org/10.1146/annurev-anthro-010220-074429

Purba, I. G. & Can, S. (2016). Legal study on the crime of defamation through social media according to law number 19 of 2016 concerning information and electronic transactions. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *5*(19), 10240–10251.

Puspitasari, I. (2018). Pertanggungjawaban pidana pelaku tindak pidana penipuan online dalam hukum positif di Indonesia. *Humani (Hukum dan Masyarakat Madani)*, *8*(1), 1–14. https://doi.org/10.26623/humani.v8i1.1383

Putri, R. N. S. (2022). *Analisa pola – pola sosialisasi pencegahan modus social engineering oleh bank melalui media website dan media sosial Twitter*. https://dspace.uii.ac.id/handle/123456789/41513

Sabina, D., Dewi, D. A. & Hayat, R. S. (2023). Implementasi literasi budaya dan kewarganegaraan sebagai solusi disinformasi pada masyarakat Indonesia. *Jurnal Pendidikan Indonesia (JOUPI)*, *1*(3), 295–230. https://doi.org/10.62007/joupi.v1i3.219

Saifudin, A. (2024). Language communication in the digital era in the perspective of cognitive linguistics. *Proceedings of International Seminar on Translation, Applied Linguistics, Literature, and Cultural Studies*, *2*(1), 253–258. https://doi.org/10.33633/STRUKTURALJOURNAL.V2I1.12307

Salloum, S., Gaber, T., Vadera, S. & Shaalan, K. (2023). A new English/Arabic parallel corpus for phishing emails. *ACM Transactions on Asian and Low-Resource Language Information Processing*, *22*(7), 1–17. https://doi.org/10.1145/3606031

Santoso, J. T. (2023). *Teknologi keamanan siber (Cyber Security)*. *9*(1), 1–173.

Strada, Y. A., Donoriyanto, D. S. & Rahmawati, N. (2022). Cash information system design based on website (Case study on Café XYZ). *Tibuana*, *5*(2), 99-106. https://doi.org/10.36456/tibuana.5.2.5594.99-106

Taufiq, M., Maliki, D. O., Maldini, A. S., Ekamartha, K. N., Saputra, K. N. C., Ahmad, S. H., Pillardien, E. & Sholihatin, E. (2023). Pentingnya Etika berbahasa sebagai upaya pencegahan kasus kejahatan berbahasa di media digital. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, *3*(2), 2116–2125. https://doi.org/10.53363/bureau.v3i2.311

Tomicic, I. (2023). Social engineering aspects of email phishing: An overview and taxonomy. *2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings*, 1201–1207. https://doi.org/10.23919/MIPRO57284.2023.10159691

Wallis, P. (2022). An enactivist account of mind reading in natural language understanding. *Multimodal Technologies and Interaction*, *6*(5), 32. https://doi.org/10.3390/mti6050032

Warami, H. (2022). Kejahatan bahasa di wilayah hukum Papua Barat: Kajian linguistik forensik. *Ranah: Jurnal Kajian Bahasa*, *11*(1), 76–93. https://doi.org/10.26499/rnh.v11i1.2699

Weaver, B. W., Braly, A. M. & Lane, D. M. (2021). Training users to identify phishing emails. *Journal of Educational Computing Research*, *59*(6), 1169–1183. https://doi.org/10.1177/0735633121992516