Jurnal Kemitraan Masyarakat
Volume 2, Nomor 2, Juni 2025
e-ISSN: 3032-5994; p-ISSN: 3032-6001, Hal. 159-167
DOI: https://doi.org/10.62383/jkm.v2i2.1596
Available online at: https://pkm.lpkd.or.id/index.php/JKM

Ancaman dan Pencegahan *Phishing* Pengguna Media Sosial untuk Siswa di SMK Wisata Indonesia

Threats and Prevention of Phishing Social Media Users for Students at SMK Wisata Indonesia

Andri[1], Somawati[2*]
[1-2]Universitas Indraprasta PGRI, Jakarta, Indonesia

**Korespondensi penulis: somadasay@gmail.com*

Article History:
Received: Mei 11, 2025;
Revised: Mei 29, 2025;
Accepted: Juni 14, 2025;
Published: Juni 17, 2025

Keywords: *Cyber Security, Phishing, Social Media.*

Abstract: *In these modern days, it is very difficult to find a person who is far from the internet or from their smartphone devices. The phenomenon that arises is that almost everyone now has more than one social media account. Social media itself, besides functioning as a space for socializing, is also used as a business platform, like online stores, due to the increasing number of users. However, when this opportunity exists, cybercriminals also prowl in search of easy ways to profit from unsuspecting users. One of the methods they rely on is phishing techniques. Phishing is a scenario designed to deceive people into unknowingly handing over their personal data to the trapper. By providing education about threats and ways to prevent this type of attack on social networking platforms, it is hoped that the public can become more critical and suspicious of suspicious signs on accounts or other web pages, as well as take appropriate preventive measures.*

Abstrak

Dihari-hari modern ini, sulit sekali menemukan orang yang jauh dari internet atau dari perangkat ponsel pintarnya. Fenomena yang muncul adalah hampir setiap orang kini memiliki lebih dari satu akun media sosial. Media sosial itu sendiri, selain berfungsi sebagai ruang bersosialisasi, juga dijadikan lahan berbisnis, seperti toko daring, karena jumlah pengguna yang terus membengkak. Namun, ketika peluang itu ada, penjahat siber pun bergerilya mencari cara meraih untung yang mudah dari para pengguna yang lengah. Salah satu metode yang mereka andalkan adalah teknik phishing. Phishing adalah skenario yang dirancang untuk mengelabui orang hingga ia secara tidak sadar menyerahkan data pribadinya kepada si penjebak. Dengan memberi edukasi tentang ancaman dan cara mencegah serangan ini di platform jejaring sosial, diharapkan khalayak dapat lebih kritis dan curiga terhadap tanda-tanda mencurigakan di akun atau laman web lain, serta melakukan langkah-langkah pencegahan yang tepat.

Kata Kunci: Keamanan Siber, Media Sosial, Phishing.

1. PENDAHULUAN

Di zaman serba nyata dan digital saat ini, hampir tidak mungkin seseorang terpisah dari internet dan perangkat pintar yang terus menyala (Isyanto et al., 2022). Ditambah lagi, banyak orang berlomba-lomba memperbanyak akun di situs jejaring sosial demi menarik perhatian publik, entah itu di Facebook, Twitter, Instagram, Snapchat, atau platform baru lainnya (Syaripudin and Badruzzaman 2022). Untuk mendapatkan berita terbaru, pengguna tinggal menelusuri beragam artikel lokal maupun internasional yang diunggah di laman web atau langsung muncul di beranda media social (Mardiana, Utomo, and Amaliah 2022). Sebelum

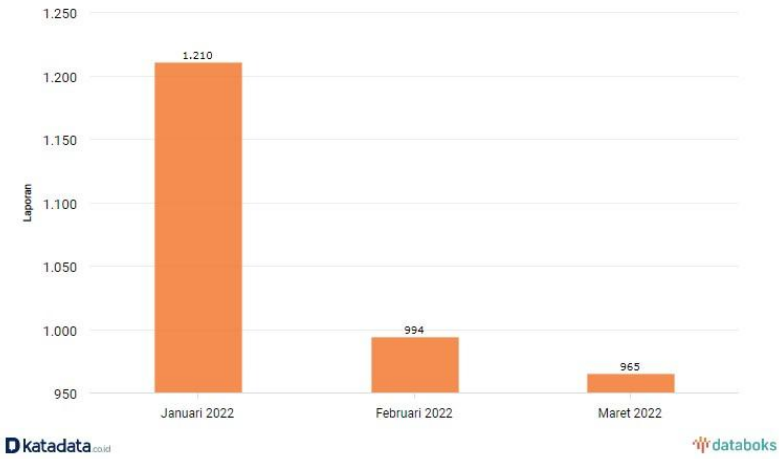
semua itu dapat dijangkau, tentu saja setiap pengguna lebih dahulu membuka peramban, pintu gerbang menuju lautan jejaring digital. Tidak jarang, satu orang pun memiliki dua, tiga, bahkan belasan akun di berbagai ruang maya yang berbeda (Putu Hendika Permana 2021). Selain sebagai arena bersosialisasi, platform-platform ini juga berfungsi sebagai pasar virtual di mana toko daring, atau online shop, dapat tampil tanpa perlu memiliki etalase fisik (Triyani Capeg Hadmandho 2022). Prosesnya terbilang simpel dan cukup menguntungkan, sebab modal awal yang besar tidak selalu diperlukan; pedagang hanya perlu mengunggah foto produk dan menulis deskripsi singkat (Fardiansyah et al. 2022). Pembayaran pun fleksibel, bisa ditransfer melalui rekening, diambil langsung saat barang sampai, atau lewat fasilitas pasar online lainnya (Fatman, Khoirun Nafisah, and Bendoro Jembar Pambudi 2023).

Ketika jumlah pengguna media sosial terus melejit di seluruh dunia, para penjahat siber pun tidak tinggal diam, mereka mencari celah untuk meraup keuntungan dari orang-orang yang percaya diri beraktivitas di dunia maya (Syah 2023). Salah satu strategi yang paling umum mereka terapkan adalah phising (Butarbutar 2023). Phishing dalam bahasa awam bisa digambarkan sebagai jebakan yang sengaja dibuat untuk 'memancing' korbannya agar mau menyerahkan data pribadi (Alkhalil et al. 2021; Zieni, Massari, and Calzarossa 2023). Penipu hanya perlu mendesain pesan atau laman yang tampak resmi (Rian Handoko and Tata Sutabri 2023), sehingga korban tanpa sadar mengetikkan kata sandi, nomor rekening, atau informasi penting lainnya. Karena modus ini menggunakan sarana internet, phishing digolongkan sebagai kejahatan siber yang jumlahnya terus melambung seiring pertumbuhan penggunaan komputer dan smartphone. Seiring waktu, teknik kriminal di dunia maya terus beradaptasi dan menyebar ke hampir setiap negara (Sudiyawati and Mertha 2022). Bagi peretas, meluncurkan kampanye pishing terasa relatif mudah dan murah, sehingga orang-orang yang lengah tetap terperangkap. Keberadaan celah pendidikan di ruang digital ini menunjukkan, meski ancaman tampak remeh, rasa percaya diri yang berlebihan tetap dapat membuat siapapun menjadi mangsa.

Banyak pengguna media sosial sama sekali tidak menimbang ancaman semacam itu (Putri et al. 2022). Mereka menganggapnya sepele dan tidak layak diributkan. Hingga detik ini, ratusan ribu akun sudah terjerat umpan pancing (Vadila and Pratama 2021). Salah satu modus yang sering dipakai penjahat siber ialah menempelkan tautan palsu di postingan, lengkap dengan ajakan atau iklan yang tampak megah dan menggoda (Purwani 2023). Melalui tautan itu, pelaku bisa mengumpulkan data pribadi lalu mengeksploitasinya, misalnya menguras saldo rekening atau memakai akun untuk belanja daring. Langkah pencegahan paling sederhana adalah membiarkan tautan tak dikenal, baik yang masuk lewat media sosial maupun lewat surel, tanpa diklik (Wiatma Jonimandala, KGSondakh, and Sondakh 2023). Tautan yang asing

patut dicurigai sebab ia bisa menjadi perangkap yang kemudian menyebarkan virus serupa ke seluruh jaringan pengguna lain.

Sesungguhnya, sosialisasi yang digelar ini bertujuan pertama-tama untuk mendorong setiap orang mengubah cara pikirnya tentang ancaman phishing (Hadi Ramadhan and Kumalasari Nurnawati 2022). Kemudian, peserta perlu dilatih mengenali tanda-tanda mencurigakan pada akun media sosial maupun situs web lainnya. Apabila memang ditemukan halaman palsu, mereka harus segera meninggalkannya tanpa ragu-ragu. Namun, pergi saja tidak cukup; kita juga wajib mencari langkah penyelamatan agar akun tetap aman. Hal ini berarti mencari dan memasang perangkat antiphishing yang tepat sebelum kerusakan semakin meluas (Varshney et al. 2024). Sebab, sekali terserang, ancaman tersebut biasanya menyebar ke kontak-kontak lain dalam sekejap. Virus digital ini terus melaju dari satu layar ke layar lain, menjelajahi seluruh dunia maya. Dalam lingkaran jejaring sosial, pengguna yang terinfeksi sering kali tidak sadar, sementara teman-temannya marah karena tiba-tiba menerima pesan spam tanpa henti. Tidak ada kepastian kapan serangan mitra peretas akan berhenti, sebab mereka selalu melahirkan trik baru untuk mengganggu aktivitas online. Malangnya, setiap tahun angka kasus terus merangkak naik dan korban yang terjaring sudah tidak mungkin lagi cukup dihitung dengan jari.



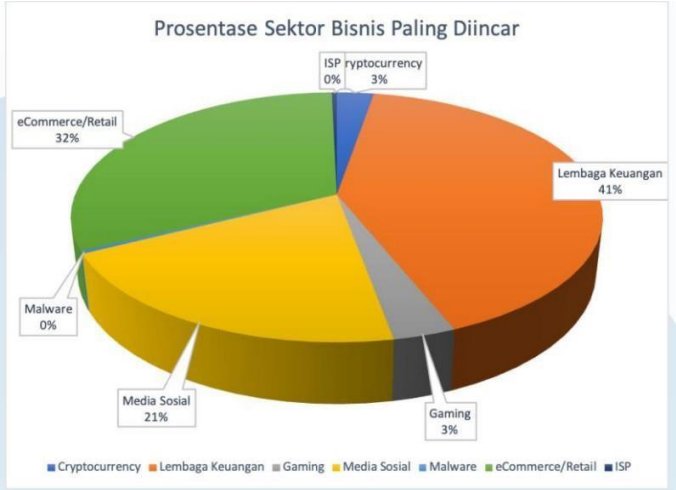
Gambar 1. Laporan Kejahatan *Phishing* Tahun 2022

Badan Anti-Phishing Indonesia, yang dikenal sebagai IDADX, mencatat sebanyak 3.180 laporan serangan phishing selama kuartal pertama 2022 (Sekar et al. 2024). Angka tersebut menunjukkan penurunan dibanding kuartal keempat 2021 yang mencapai 5.325 laporan. Namun, bila diukur dengan periode yang sama tahun lalu, jumlah tersebut sebenarnya meningkat, sebab pada kuartal pertama 2021 IDADX hanya menerima 536 pengaduan. Pada

periode Januari-Maret 2022, bulan Januari mencatat angka tertinggi, yaitu 1.210 laporan, sementara Februari dan Maret masing-masing turun menjadi 994 laporan dan 965 laporan. Organisasi yang menjadi sasaran phishing juga tercatat sebanyak 58 entitas, disertai 125 nama domain yang dipakai pelaku sepanjang Januari hingga Maret. Beberapa nama besar yang tercantum dalam daftar target serangan itu antara lain Internal Revenue Service (IRS), Microsoft, Crypto, PayPal, dan Amazon.

Sebagian orang memperolehkannya dengan cara yang terbilang gampang. Mereka tidak selalu mengejar uang semata-mata (Muftiadi, Agustina, and Evi 2022). Terkadang niat utama sekadar bersenang-senang atau mengintip aktivitas pemilik akun. Apabila beruntung, sekaligus uang mampir dan isi profil lawan serangnya tampak. Bila sasaran hanya individu biasa, masalah biasanya cepat reda dan tanpa konsekuensi berat. Namun, bagaimana jika objek serangan adalah tokoh penting atau figur berpengaruh global? Peristiwa semacam itu bukan barang baru di dunia maya. Banyak pemimpin puncak ternyata ikut terlibat, meski berperan sebagai penyuruh saja. Aktivitas itu kemudian dikerjakan oleh para hacker yang siap mengeksekusi perintah. Kejadian serupa sudah lazim, terutama pada masa kampanye politik (Mohd. Yusuf DM et al. 2022). Dua perusahaan yang tadinya bersahabat pun bisa berbalik, setelah satu pihak merasa bagian laba tidak sesuai kesepakatan.

Pusat Pemantauan ID-IDX, lembaga anti-phising Indonesia, menerima 5.579 pengaduan phising buat kuartal II-2022. Angka itu melejit 1.637 laporan dibandingkan kuartal I-2022 yang masih rendah.



Gambar 2. Prosentase Sektor Bisnis yang Paling Diincar Kejahatan *Phishing*

Berdasarkan grafik di atas, sektor media sosial pada kuartal kedua menyumbang 21 persen, posisi ketiga setelah dua sektor lain, sehingga media sosial patut mendapat perhatian ekstra, terutama karena banyak remaja aktif di sana dan rentan terhadap phising.

Munculnya tawaran untung cepat sering menembus nurani bisnis sehat dan melahirkan rencana curang. Para pelaku itu lalu memanfaatkan hacker sebagai mata pisau untuk menghancurkan pesaing (Chng et al. 2022). Mereka memerintah si hacker menyusup, mencuri data keuangan lawan, lalu merapikan dan memanipulasinya hingga tampak sah. Setelah permainan selesai, seluruh uang hasil pengalihan itu dialihkan kepada perusahaan penyewa jasa jahat itu. Sebagai imbalan, hacker itu menerima potongan kecil, biasanya beberapa persen dari total yang diambil. Meski kejahatan semacam ini menggiurkan, masih banyak orang baik yang terus berkarya menciptakan alat deteksi dan aplikasi pencegah. Kebanyakan peneliti dan pengembang tersebut dulunya adalah korban serangan phishing, sehingga mereka merasa sakit hati. Ketidakpuasan itu mendorong mereka membalas dengan menciptakan solusi anti-phishing yang lebih cerdas dan handal (Jampen et al. 2020).

Karena itu, setiap orang harus memanfaatkan pengetahuan tersebut agar risiko serangan phishing bisa berkurang (Ginting et al. 2023). Jika seseorang merasa langkah-langkah pencegahan terlalu merepotkan, ia tetap dapat melindungi akunnya dengan pengaturan keamanan yang tepat. Hanya melalui usaha tersebut sebuah akun bisa aman, dan penggunanya dapat bersosialisasi di dunia maya dengan nyaman. Dengan kata lain, program pengabdian kepada masyarakat ini bertujuan memperkenalkan cara dasar mencegah serangan phishing di media sosial dan mengetahui respon siswa-siswi setelah menerima edukasi ancaman tersebut.

2. METODE PENELITIAN

Pengabdian kepada masyarakat ini ditujukan kepada siswa-siswi SMK Wisata Indonesia dan pelaksanaannya berlangsung di ruang kelas sekolah tersebut pada pukul 10.00. Tim pengabdian menggunakan beberapa metode, yaitu presentasi materi, sesi tanya jawab, diskusi, serta praktik langsung (Susi and Yasir 2021), dan seluruh penyampaian didukung media PowerPoint agar slide materi dapat dilihat dan dipahami dengan jelas oleh peserta. Setelah pemaparan, para siswa diberikan kesempatan bertanya, sehingga mereka dapat memastikan setiap penjelasan dari tim pengabdian benar-benar dipahami dengan baik.

Dalam kegiatan PKM kali ini, kerja sama berlangsung langsung antara tim PKM Universitas Indraprasta PGRI Jakarta dan pihak sekolah, tanpa melibatkan sponsor atau mitra lain. Jika pelaksanaan berjalan mulus, tim akan menjajaki dukungan dari pihak ketiga untuk kegiatan PKM mendatang.

Berikut langkah-langkah yang kami usulkan untuk menjalankan solusi dan menyelesaikan masalah yang ada:

1) Ketua tim bekerja sama dengan kepala sekolah SMK Wisata Indonesia agar sekolah bisa menggelar penyuluhan tentang ancaman dan cara mencegah phising di media sosial bagi seluruh siswa.
2) Tim persiapan lalu menyiapkan semua alat dan fasilitas yang dibutuhkan, seperti ruang acara, proyektor, handout, serta sarana logistik lain.
3) Saat acara berlangsung, narasumber menyampaikan materi dasar ancaman phising dan langkah-langkah pencegahannya dengan cara yang mudah dimengerti oleh siswa.
4) Setelah itu, narasumber memberikan penjelasan lebih dalam, menjawab pertanyaan, dan memberi contoh nyata agar siswa benar-benar paham dan waspada.

Pelaksanaan penyuluhan program PKM direncanakan dihadiri minimal dua puluh peserta. Setelah acara berlangsung, tim PKM akan langsung mengevaluasi kegiatan guna memastikan program berjalan sesuai rencana. Apabila hasil awal belum memuaskan, tim itu akan memperbaiki setiap pertemuan dan berupaya sekuat tenaga agar seluruh proses tetap lancar.

3. HASIL DAN PEMBAHASAN

Setelah mengikuti kegiatan pengabdian bertajuk Ancaman dan Pencegahan Phishing bagi pengguna media sosial, siswa-siswi SMK Wisata Indonesia kini lebih memahami sifat bahaya serta langkah-langkah pencegahan serangan phishing di platform-platform sosial tersebut.

Gambar 3. Kegiatan Saat PKM Berlangsung

Gambar 4. Dokumentasi Saat Kegiatan Dilaksanakan

Karena itu, setiap orang perlu memanfaatkan semua tips keamanan supaya risiko ditipu lewat email palsu bisa berkurang. Kalau merasa langkah-langkah itu repot, setidaknya pasang sandi kuat dan aktifkan verifikasi dua langkah. Dengan begitu, akun tetap aman dan kita bisa bersosialisasi di dunia maya tanpa khawatir kehilangan data.

4. KESIMPULAN

Berdasarkan seluruh rangkaian kegiatan yang telah dilaksanakan, dapat disimpulkan bahwa pengetahuan siswa-siswi SMK Wisata Indonesia tentang ancaman serta langkah pencegahan phishing di platform media sosial telah mengalami peningkatan yang signifikan. Setelah mengikuti seminar, para siswa diharapkan mampu mengidentifikasi berbagai bentuk ancaman phishing serta dapat menerapkan langkah-langkah pencegahan secara mandiri saat berinteraksi di dunia maya.

DAFTAR REFERENSI

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*. https://doi.org/10.3389/fcomp.2021.563060

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Jurnal Hukum & Pembangunan, 2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*. https://doi.org/10.1016/j.chbr.2022.100167

Fardiansyah, M., Nur, A. W., Arief, A., & Hizbullah, I. (2022). Agile Scrum untuk platform e-commerce UMKM kuliner: Studi kasus toko. *Jurnal Pedimas Pasifik, 1*(1).

Fatman, Y., Nafisah, N. K., & Pambudi, P. B. J. (2023). Implementasi payment gateway dengan menggunakan Midtrans pada website UMKM Geberco. *Jurnal KomtekInfo*. https://doi.org/10.35134/komtekinfo.v10i2.364

Ginting, E., Sinaga, M. P., Nurdin, M. R., & Putra, M. D. (2023). Analisis ancaman phishing terhadap layanan online perbankan (Studi kasus pada Bank BRI). *UNES Journal of Scientech Research*.

Hadi Ramadhan, I., & Nurnawati, E. K. (2022). Analisis ancaman phishing dalam layanan e-commerce. *Prosiding SNAST, 8*(1). https://doi.org/10.34151/prosidingsnast.v8i1.4169

Handoko, R., & Sutabri, T. (2023). Analisa machine learning dengan algoritma multi-layer perceptron untuk penanganan kejahatan phishing. *Jurnal Informatika Teknologi dan Sains, 5*(1). https://doi.org/10.51401/jinteks.v5i1.2221

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*. https://doi.org/10.1186/s13673-020-00237-7

Mardiana, N. Y., Utomo, N. A., & Amaliah, Y. R. (2022). Pengaruh persepsi kegunaan dan kemudahan teknologi internet terhadap efektivitas perusahaan di JABODETABEK. *Ekonomika, 6*.

Mohd. Yusuf, D. M., Yola, V., Maiharani, D., & Dwi, E. (2022). Analisis terhadap modus-modus dalam hukum cyber crime. *Jurnal Hukum, Politik dan Ilmu Sosial, 1*(2). https://doi.org/10.55606/jhpis.v1i2.725

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

Permana, P. H., & Sutedja, D. M. (2021). Analisis perilaku pengguna akun kedua di media sosial Instagram. *Jurnal Inovasi Penelitian, 2*(4).

Purwani, M. S. F. (2023). Analisis peran dan penanggulangan kejahatan siber: Studi kasus spearphishing. *Restorative: Journal of Indonesian Probation and Parole System, 1*(1). https://doi.org/10.61682/restorative.v1i1.5

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan hacking tools sebagai ancaman siber dalam sistem pertahanan negara (Studi kasus: Predator). *Global Political Studies Journal, 6*(1). https://doi.org/10.34010/gpsjournal.v6i1.6698

Sekar, A., Umami, N., Lutfi, A. M., Kusumawati, A., Hayyu, D., Muna, R., & Ningsih, T. D. (2024). Efektivitas strategi kampanye iklan edukasi Bank BCA 'Don't Know? Kasih No!' terhadap maraknya fenomena phishing di masyarakat. *Jurnal Ekonomi Manajemen dan Akuntansi, 2*.

Sudiyawati, N. P. L., & Mertha, I. K. (2022). Kejahatan siber (cybercrime) dalam konteks kekerasan seksual berbasis gender online di Indonesia. *Kertha Semaya: Journal Ilmu Hukum, 10*(4). https://doi.org/10.24843/ks.2022.v10.i04.p11

Susilawati, S., & Yasir, M. (2021). Transformasi media pembelajaran di masa pandemi Covid-

19. *Literasi: Jurnal Pengabdian Masyarakat dan Inovasi, 1*(2). https://doi.org/10.58466/literasi.v1i2.91

Syah, R. (2023). Strategi kepolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. *Jurnal Impresi Indonesia, 2*(9). https://doi.org/10.58344/jii.v2i9.3594

Syaripudin, E. I., & Badruzzaman, P. (2022). Jual beli followers di media sosial Instagram tentang transaksi elektronik dalam pandangan hukum Islam. *Jurnal Hukum Ekonomi Syariah (JHESY), 1*(1). https://doi.org/10.37968/jhesy.v1i1.170

Triyani Capeg Hadmandho. (2022). Pengaruh keyakinan pada toko daring terhadap perilaku pembelian impulsif konsumen online. *Hirarki: Jurnal Ilmiah Manajemen dan Bisnis, 4*(1). https://doi.org/10.30606/hirarki.v4i1.1467

Vadila, N., & Pratama, A. R. (2021). Analisis kesadaran keamanan terhadap ancaman phishing. *Automata, 2*(2).

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2023.122199

Wiatma Jonimandala, G., Sondakh, D. K. G., & Sondakh, J. (2023). Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskrim Polri dalam melakukan penegakan hukum terhadap kejahatan pencurian dan penyalahgunaan data pribadi. *Journal of Social Science Research, 3*(4).

Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or not phishing? A survey on the detection of phishing websites. *IEEE Access, 11*. https://doi.org/10.1109/ACCESS.2023.3247135