Jurnal Impresi Indonesia (JII)
Vol. 2, No. 9, September 2023
p-ISSN: 2828-1284 e-ISSN: 2810-062x
website: https: //rivierapublishing.id/JII/index.php/jii/index

STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER

Rahmat Syah
Sekolah Tinggi Ilmu Kepolisian
rahmat.syah.1620@gmail.com

Keywords
Policing, Phishing and Social Media Strategies

Abstract
Phishing crimes via social media in cyber space are a serious threat in the ever-growing digital world. This research aims to examine policing strategies in preventing phishing crimes via social media. A qualitative approach was used in this research to understand the complex issues related to phishing attacks and involved the perspective of social media users. The research results show that cybercriminals are increasingly clever in utilizing social media to launch phishing attacks by posing as trusted entities. This research highlights the lack of user awareness and understanding of the risks of phishing and the need for education about the signs of an attack and how to protect yourself. Additionally, this research highlights the psychological factors exploited by cybercriminals in phishing attacks. So a holistic and collaborative policing strategy is needed to create a cyber environment that is safer and protected from increasingly complex phishing attacks in this digital era by collaborating between authorities and social media platforms in overcoming phishing threats, which is also supported by user-based policing. Also has an important role. Another strategy that can be used is providing education and outreach regarding user understanding in preventing phishing crimes which can be supported by the use of technology.

Kata Kunci
Startegi Pemolisian, Phishing dan Media Sosial

Abstrak
Kejahatan phising melalui media sosial di ruang siber merupakan ancaman serius dalam dunia digital yang terus berkembang. Penelitian ini bertujuan untuk mengkaji strategi pemolisian dalam pencegahan kejahatan phising melalui media sosial. Pendekatan kualitatif digunakan dalam penelitian ini untuk memahami isu-isu kompleks yang terkait dengan serangan phising dan melibatkan perspektif pengguna media sosial. Hasil penelitian menunjukkan bahwa penjahat siber semakin cerdik dalam memanfaatkan media sosial untuk melancarkan serangan phising dengan menyamar sebagai entitas tepercaya. Penelitian ini menggarisbawahi kekurangan kesadaran dan pemahaman pengguna tentang risiko phising serta perlunya pendidikan tentang tanda-tanda serangan dan cara melindungi diri. Selain itu, penelitian ini menyoroti faktor psikologis yang dimanfaatkan oleh penjahat siber dalam serangan phising. Sehingga strategi pemolisian yang holistik dan kolaboratif diperlukan untuk menciptakan lingkungan siber yang lebih aman dan terlindungi dari serangan phising yang semakin kompleks di era digital ini dengan cara kolaborasi antara pihak berwenang dan platform media sosial dalam mengatasi ancaman phising, yang didukung pula dengan pemolisian berbasis pengguna juga memiliki peran penting. Strategi lain yang dapat digunakan yaitu mengadakan edukasi dan penyuluhan tentang pemahaman pengguna dalam pencegahan kejahatan phishing yang dapat didukung dengan pemanfaatan teknologi.

Corresponding Author: Rahmat Syah
E-mail: rahmat.syah.1620@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi, khususnya dalam penggunaan media sosial telah menjadi bagian integral dari kehidupan sehari-hari yang memungkinkan orang untuk berinteraksi, berbagi informasi, dan menjalankan berbagai aktivitas. Perkembangan teknologi diikuti dengan munculnya tindak pidana baru juga. Di dalam dunia nyata, seseorang dapat masuk ke rumah milik orang lain dan mengambil barang berharga di rumah orang tersebut, apabila di dunia maya seseorang dapat mengakses komputer atau jaringan komputer milik orang lain dan mengambil data berharga milik orang lain (Arfah, 2020).

Di jaman Era Globalisasi ini segala sesuatu aspek kehidupan yang ada bersaing begitu ketatnya. Dari mulai aspek ekonomi, politik, sosial budaya, pendidikan dan lain-lain. Kondisi kehidupan telah mengalami perbaikan, secara bersamaan telah menciptakan suatu jurang perbedaan yang dalam antara orang-orang yang hidup di negara-negara maju dengan orang-orang yang hidup di negara yang sedang berkembang dan negara-negara terbelakang (Hasan & Azis, 2018). Dalam era seperti sekarang ini, ketika dunia dihadapkan pada ketidakpastian dan ketidakmenentuan (*turbulance and uncertainty*), teknologi informasi yang semakin canggih, masyarakat yang semakin berani dengan beragam tuntutannya, dan persaingan yang semakin ketat (Pasaribu & Widjaja, 2022). Munculnya berbagai tekanan dan tantangan atau bahkan ancaman dari berbagai arah terhadap negara.

Peran media sosial sebagai saluran utama bagi individu dan bisnis untuk berkomunikasi, berkolaborasi, dan berinteraksi dengan masyarakat menjadikan kerentanannya terhadap serangan phishing. Phishing adalah taktik yang umum digunakan oleh penjahat siber untuk memperoleh informasi pribadi dengan menyamar sebagai entitas tepercaya (Sutarli & Kurniawan, 2023). Melalui media sosial, serangan phishing semakin populer, memanfaatkan ketidakwas-wasan pengguna terhadap potensi risiko. Serangan semacam ini dapat memiliki dampak serius pada individu dan organisasi, seperti pencurian identitas, kebocoran data sensitif, dan kerugian keuangan. Kebocoran informasi pribadi dan kerugian finansial yang dapat ditimbulkan oleh serangan ini dapat merusak kepercayaan dan stabilitas di dunia maya.

Terlebih lagi, kekhawatiran akan penyebaran informasi palsu atau hoaks melalui media sosial juga menjadi isu yang tak terpisahkan dari masalah ini. Serangan phishing sering kali melibatkan penyebaran tautan atau informasi palsu yang dapat dengan mudah menipu pengguna (Simarmata, Iqbal, Hasibuan, Limbong, & Albra, 2019). Penjahat siber terus berinovasi dan mengembangkan teknik-teknik baru untuk melancarkan serangan phishing yang lebih canggih dan menipu. Masalah ini memiliki implikasi yang lebih luas dalam konteks keamanan siber dan perangkat lunak keamanan. Perkembangan teknologi keamanan siber perlu terus dipantau dan disesuaikan untuk menghadapi ancaman phishing yang semakin kompleks.

Kekurangan pemahaman dan kesadaran tentang cara mengidentifikasi tanda-tanda serangan phishing juga menjadi masalah yang perlu dibereskan. Banyak pengguna media sosial mungkin tidak tahu cara melindungi diri mereka sendiri dan bagaimana cara berperilaku secara aman di dunia maya. Di sisi lain, media sosial memiliki peran penting dalam mendukung kehidupan sosial dan bisnis, sehingga melarang atau membatasi penggunaannya bukanlah solusi yang realistis. Oleh karena itu, perlu adanya strategi pemolisian yang efektif untuk menjaga keamanan di platform media sosial.

Ancaman ini dapat mengancam kestabilan dan keamanan serta ketahanan nasional sehingga perlu mendapat perhatian khusus dalam menghadapinya sesuai dengan tingkat dan pola ancaman yang dilakukan. Polisi sebagai lembaga pemerintah yang didirikan untuk menyelenggarakan tugas mewujudkan dan memelihara keteraturan sosial. Penyelenggaraan tugasnya adalah memberikan perlindungan, pengayoman dan pelayanan, serta penegakkan hukum dan menyelenggarakan tugasnya melalui pemolisian. Pemolisian adalah segala usaha yang dilakukan polisi pada tingkat manajemen maupun tingkat operasional, dengan atau tanpa upaya paksa, dalam mewujudkan dan memelihara kamtibmas

Tantangan dalam penerapan kepolisian terhadap penipuan siber di Indonesia dapat menjadi tantangan dikategorikan menjadi masyarakat, penjahat, dan pemerintah. Dari segi

masyarakat, mayoritas adalah disebabkan oleh kurangnya kesadaran dan rendahnya tingkat literasi dalam memahami kejahatan dunia maya khususnya penipuan daring. Dari segi pelakunya, selain sifat kejahatannya yang tidak mengenal batas, juga Pelaku sudah "selangkah lebih maju" dengan melakukan kejahatan jenis baru sebelumnya pemerintah dapat memperkenalkan peraturan. Registrasi kartu SIM, misalnya, ditujukan untuk mencegah kejahatan namun malah menjadi wadah baru untuk melakukan kejahatan jual beli identitas oleh pelaku sebelum adanya hukum.

Dengan mengidentifikasi dan memahami latar belakang masalah ini, penelitian tentang strategi pemolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber akan menjadi langkah penting dalam melindungi masyarakat dan organisasi dari potensi bahaya yang mengintai di dunia digital yang terus berkembang ini. Selain itu, penelitian ini dapat memberikan kontribusi berharga dalam merancang kebijakan dan pedoman untuk meningkatkan keamanan dan privasi pengguna media sosial, sekaligus mempromosikan perilaku cyber yang aman dan bertanggung jawab.

METODE PENELITIAN

Metodologi penelitian yang digunakan dalam studi ini adalah pendekatan kualitatif, yang akan menggali pemahaman mendalam tentang permasalahan keamanan siber dalam konteks media sosial. Penelitian ini akan melibatkan berbagai tahapan, termasuk pengumpulan, analisis, dan interpretasi data kualitatif. Pengumpulan data akan dilakukan melalui teknik-teknik seperti wawancara mendalam dengan pengguna media sosial, analisis konten dari postingan dan tau tan yang berpotensi berbahaya, serta observasi langsung dalam lingkungan media sosial. Data yang diperoleh akan dianalisis secara tematis untuk mengidentifikasi pola, tren, dan temuan penting yang berkaitan dengan pengalaman pengguna, perilaku penjahat siber, serta upaya pencegahan yang telah dilakukan. Analisis kualitatif ini berguna untuk memahami konteks sosial, budaya, dan psikologis yang mendasari isu keamanan siber ini, serta merumuskan rekomendasi strategis yang relevan untuk meningkatkan pemolisian dan kesadaran masyarakat terhadap phishing di media sosial.

HASIL DAN PEMBAHASAN

Hasil penelitian ini memberikan wawasan yang penting mengenai strategi pemolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. Penipuan siber adalah suatu bentuk penipuan yang memanfaatkan media internet dan komputer dalam pelaksanaannya. Sejalan dengan klasifikasi dari peneliti yang menyebutkan kejahatan siber berhubungan dengan komputer atau internet kejahatan jaringan sebagai perantara kejahatan konvensional (Suhaemin & Muslih, 2023). Oleh karena itu, yang menjadikan kejahatan siber menarik untuk dibahas adalah karena penipuan siber memiliki perbedaan karakteristik dibandingkan dengan kejahatan dunia maya lainnya karena fitur anonim kompleks yang disediakan melalui internet menyediakan (Suhaemin & Muslih, 2023). Oleh karena itu, korban cenderung tidak melaporkan kejahatannya kepada pihak berwenang karena rasa malu yang dirasakan karena menjadi korban penipuan dunia (Suhaemin & Muslih, 2023), dan kesulitan untuk mengidentifikasi pelakunya (Buchanan & Whitty, 2014).

Berdasarkan data dan analisis kualitatif yang telah dilakukan, beberapa temuan signifikan hasil wawancara dengan seorang responden dalam konteks penelitian mengenai strategi pemolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. Responden ini adalah seorang pengguna media sosial yang aktif dan memiliki pengalaman terkait dengan phishing di platform media sosial.

"Saya pernah mengalami situasi seperti itu. Saya menerima sebuah pesan di DM (Direct Message) dari seseorang yang mengaku menjadi teman lama saya. Mereka meminta informasi pribadi saya, seperti alamat email dan kata sandi, dan berusaha meyakinkan saya bahwa mereka membutuhkannya untuk alasan tertentu. Awalnya, saya hampir saja memberikan informasi tersebut karena saya percaya mereka adalah teman lama saya. Tapi kemudian, sesuatu terasa aneh, dan saya memutuskan untuk tidak memberikan informasi

itu. Saya kemudian menghapus pesan tersebut dan memberi tahu teman sebenarnya bahwa akun mereka mungkin telah diretas".

Hasil penelitian menunjukkan bahwa penjahat siber semakin cekatan dalam memanfaatkan media sosial sebagai sarana untuk menjalankan serangan phishing. Mereka seringkali menggunakan akun palsu yang menyamar sebagai entitas tepercaya, seperti bank atau perusahaan terkenal, untuk memancing korban. Hal ini menekankan pentingnya upaya pemolisian dan identifikasi akun palsu di platform media sosial. Salah satu tantangan utama adalah ketidakpastian. Seringkali, pesan phishing ini terlihat sangat meyakinkan, dan sulit untuk membedakannya dari pesan asli. Selain itu, banyak pengguna media sosial mungkin tidak cukup sadar tentang ancaman ini dan cenderung mempercayai apa yang mereka lihat di platform. Penelitian ini menunjukkan bahwa serangan phishing seringkali berhasil karena penjahat siber memanfaatkan faktor-faktor psikologis, seperti rasa ingin tahu atau ketakutan. Oleh karena itu, pendekatan pemolisian juga harus mencakup aspek-edukasi psikologi yang dapat membantu pengguna menjadi lebih bijak dalam menilai tautan dan pesan yang mereka terima.

Hasil wawancara dengan seorang responden lainnya dalam strategi pemolisian mencegah kejahatan phishing melalui media sosial di ruang siber mengungkapkan

"Saya akan menyarankan kepada pengguna untuk selalu memverifikasi identitas akun yang menghubungi mereka, bahkan jika itu adalah teman lama. Jangan ragu untuk memeriksa kembali dengan mereka di luar media sosial jika Anda merasa ada sesuatu yang mencurigakan. Dan yang terpenting, selalu berpikir dua kali sebelum memberikan informasi pribadi Anda karena di lingkungan masih terdapat masyarakat yang belum memahami phishing sehingga membutuhkan edukasi dalam pencegahan phishing tersebut".

Wawancara dengan Responden memberikan wawasan yang berharga tentang pengalaman pribadi mereka dalam menghadapi upaya phishing di media sosial, serta pandangan mereka tentang strategi pemolisian dan langkah-langkah pencegahan yang efektif. Mayoritas pengguna media sosial belum sepenuhnya memahami risiko phishing di lingkungan sosial media. Mereka cenderung kurang waspada terhadap pesan atau tautan yang mencurigakan, yang dapat memudahkan penipuan. Oleh karena itu, edukasi pengguna tentang tanda-tanda serangan phishing dan cara melindungi diri adalah langkah yang sangat penting. faktor utama yang menjadi pendorong berkembangnya cyber crime adalah karena adanya Perkembangan teknologi komunikasi seperti telepon, hand phone, smart phone, gadget dan lain-lain dengan berbagai pilihan merk dan harga yang terjangkau sehingga masyarakat dapat dengan mudah untuk mengakses internet menggunakan alat teknologi tersebut. Dengan kemudahan mengakses internet tersebut namun tidak diimbangi dengan pemahaman masyarakat tentang cyber crime justru membuat masyarakat menjadi sasaran yang empuk bagi pelaku cyber crime tersebut (Suseno, 2016).

Pendidikan dianggap sebagai salah satu faktor penentu penting dalam mencegah penipuan dunia maya (Drew & Farrell, 2018). Sehingga strategi pemolisian seperti pendidikan dan kampanye kesadaran akan membantu lebih banyak orang mengerti apa itu phishing dan tanda-tandanya, mereka akan lebih waspada. Juga, penguatan keamanan akun, seperti menggunakan kata sandi yang kuat dan otentikasi dua faktor, adalah langkah-langkah yang sangat diperlukan.

Selain itu, kolaborasi antara pihak berwenang dan platform media sosial dalam mengatasi serangan phishing. Pengawasan konten menjadi salah satu komponen kunci dari strategi pemolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber. Ini mencakup langkah-langkah untuk memantau, mengidentifikasi, dan mengatasi konten yang dapat digunakan oleh penjahat siber untuk melakukan phishing. Identifikasi, tindakan preventif, dan penegakan hukum terhadap penjahat siber memerlukan kerja sama aktif dari pihak platform media sosial, termasuk pemblokiran atau penghapusan akun yang mencurigakan. Berbagai langkah dapat diambil mulai dari legislasi hingga kolaborasi dengan lembaga penegakan kejahatan dunia maya global sebagai garda terdepan dalam memerangi ancaman tersebut (Balogun & Obe, 2010).

Selain pemolisian yang dilakukan oleh pihak berwenang dan platform, pengguna juga perlu berperan aktif dalam pemolisian lingkungan media sosial. Melaporkan akun atau

aktivitas yang mencurigakan, serta berbagi pengetahuan tentang keamanan siber, dapat membantu mengurangi risiko phishing. Dalam keseluruhan, hasil penelitian ini menegaskan bahwa pencegahan kejahatan phishing melalui media sosial memerlukan strategi pemolisian yang holistik dan kolaboratif. Selain upaya teknis dan hukum, pendekatan edukasi dan kesadaran pengguna juga menjadi sangat penting. Pihak berwenang, platform media sosial, dan masyarakat luas perlu bekerja sama untuk menciptakan lingkungan siber yang lebih aman dan terlindungi dari ancaman phishing yang terus berkembang.

Selanjutnya mengatasi dampak modernisasi, teknologi dan globalisasi yang berdampak pada meningkatnya kejahatan dapat dengan membangun E-Policing. Di era digital dituntut adanya berbagai pelayanan yang serba cepat, tepat, akurat, transparan, akuntabel, informatif dan mudah diakses. Selain itu tuntutan dan harapan masyarakat terhadap kinerja polisi dalam menyelenggarakan pemolisiannya akan semakin meningkat yaitu adanya pelayanan prima. Pelayanan prima kepolisian dalam konteks ini dapat dipahami sebagai pelayanan yang cepat, tepat, akurat, transparan, akuntabel, informatif dan mudah diakses (Edithya, 2019). Penggunaan teknologi berdampak signifikan mencegah dan menyelesaikan kejahatan kriminal sehingga berkurang (Wibowo, Wangsajaya, & Surahmat, 2023).

Phishing merupakan teknik di mana penipu mencoba membuat korbannya memberikan informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dengan menyamar sebagai entitas tepercaya melalui pesan email palsu atau situs web palsu. Phishing masuk ke dalam cyber fraud yang merupakan salah satu bagian dari cybercrime juga mempunyai perbedaan dalam permasalahannya "kejahatan teritorial" yang tidak mengenal batas waktu terjadinya (Aas, 2019). Cyber fraud adalah istilah yang digunakan untuk menggambarkan tindakan penipuan atau kejahatan yang dilakukan secara online atau melalui teknologi informasi dan komunikasi. Ini adalah tindakan kejahatan yang menggunakan teknologi digital untuk merampok, meretas, atau menipu orang atau organisasi dengan tujuan mencuri uang, informasi pribadi, atau sumber daya lainnya.

Untuk meningkatkan kinerja kepolisian dalam hal pencegahan siber di Indonesia dirumuskan dengan menggabungkan praktik-praktik terbaik di negara lain dengan langkah-langkah yang ditekankan oleh teori Pencegahan Kejahatan Situasional (SCP). Oleh karena itu, diharapkan rekomendasi kebijakan yang kuat untuk pencegahan penipuan siber di Indonesia (Soesanto, Purba, Aprilia, Putra, & Putri, 2023). Misalnya, di Australia, buku strategi pencegahan khusus telah diterbitkan sebagai produk kerjasama antar instansi dan diterbitkan oleh pemerintah (Drew & Farrell, 2018). Pemerintah Indonesia harus punya strategi besar atau semacamnya buku panduan bagi masyarakat dalam mencegah penipuan yang merupakan hasil kerjasama antar kerjasama kelembagaan dan swasta.

Kebijakan Indonesia terhadap penipuan siber didasarkan pada UU ITE nomor 16 (2016). Pasal 28 angka 2 yang menggantikan UU ITE Nomor 8 Tahun 2008 pasal 28 angka 2. Pencegahan dan tugas penegakan hukum disebutkan dalam undang-undang. Polri diberi mandat untuk melakukan penyidikan dan tugas penegakan hukum, sedangkan MCT harus mengatur hukum. Meskipun berorientasi menuju teknik berorientasi masalah, penerapan kepolisian terhadap penipuan cyber di Indonesia masih perlu berbenah untuk memenuhi prinsip-prinsip kepolisian yang berorientasi pada masalah.

Peraturan perundang-undangan yang ada di Indonesia masih tetap berlaku tidak bisa mencakup seluruh permasalahan yang ada karena UU ITE tidak secara tegas mencakup data pribadi perlindungan dan penipuan. Dalam hal penerapan peraturan yang ada, pemahaman tentang anggota penegak hukum di lapangan masih dangkal. Koordinasi antar lembaga juga masih kurang institusi di Indonesia. Terdapat potensi untuk meningkatkan implementasi kepolisian mencegah penipuan siber di Indonesia dengan mengadopsi praktik terbaik dari negara lain seperti Inggris dan Australia. Secara singkat perbaikan dapat dibagi menjadi tiga bagian besar, yaitu perbaikan dan revisi peraturan, pembentukan kelembagaan dan reformasi organisasi, dan terakhir kerjasama dan kolaborasi. Dalam tahap revisi undang-undang, diperlukan regulasi mencakup terminologi penipuan dan perlindungan data pribadi. Kemudian, dalam reformasi kelembagaan tahapnya, optimalisasi lembaga-lembaga

negara untuk mengefektifkan organisasi sesuai dengan fungsinya diharapkan berfungsi dan membentuk lembaga baru yang berorientasi sebagai pusat pelaporan. Akhirnya, kerjasama dan kolaborasi antara instansi pemerintah, swasta, dan sektor sukarela untuk memberikan pencegahan yang optimal sangat diperlukan (Caroline, Kuntadi, & Pramukty, 2023).

KESIMPULAN

Pencegahan kejahatan phishing melalui media sosial memerlukan pendekatan holistik yang melibatkan berbagai pihak, termasuk pihak berwenang, platform media sosial, dan pengguna. Hanya dengan kerja sama yang kuat dan upaya bersama, dapat menciptakan lingkungan siber yang lebih aman dan terlindungi dari ancaman phishing yang terus berkembang di era digital ini. Serangan phishing melalui media sosial menjadi ancaman serius bagi individu dan organisasi, yang dapat mengakibatkan pencurian identitas, kerugian finansial, dan bahkan kerugian reputasi. Hasil penelitian ini menyoroti beberapa aspek kunci dalam upaya mengatasi masalah ini. Pertama, penelitian ini menunjukkan bahwa penjahat siber semakin cerdik dalam memanfaatkan media sosial sebagai alat untuk menjalankan serangan phishing. Akun palsu yang meniru entitas tepercaya seringkali digunakan untuk memancing korban. Oleh karena itu, upaya pemolisian yang lebih efektif dan identifikasi akun palsu di platform media sosial menjadi sangat penting. Kedua, tingkat kesadaran dan pemahaman pengguna tentang risiko phishing perlu ditingkatkan. Edukasi pengguna tentang cara mengidentifikasi tanda-tanda serangan phishing dan cara melindungi diri adalah langkah penting dalam mengurangi risiko.

Ketiga, kolaborasi antara pihak berwenang dan platform media sosial memiliki peran kunci dalam mengatasi serangan phishing. Identifikasi, pencegahan, dan penegakan hukum terhadap penjahat siber memerlukan kerja sama yang aktif. Keempat, perlunya pemolisian berbasis pengguna. Pengguna juga harus berperan aktif dalam melaporkan akun atau aktivitas mencurigakan dan berbagi pengetahuan tentang keamanan siber. Terakhir, serangan phishing seringkali berhasil karena memanfaatkan faktor-faktor psikologis pengguna. Oleh karena itu, pendekatan pemolisian juga harus mencakup aspek psikologis yang dapat membantu pengguna menjadi lebih bijak dalam menilai pesan dan tautan yang mereka terima. Selain itu, terdapat kebutuhan untuk melakukan reformasi saat ini peraturan di Indonesia. Dengan penyempurnaan undang-undang yang ada, diharapkan akan memberikan perlindungan yang lebih besar terhadap warga negara, mengurangi jumlah penipuan online, dan meningkatkan efek pencegahan pada penjahat. Indonesia perlu mendorong dan mendorong kerja sama antar institusi dan sektor lain yang berperan dalam keamanan siber.

REFERENSI

Aas, Katja Franko. (2019). Beyond 'The Desert of the Real': Crime Control in a Virtual (Ised) Reality (2006). In *Crime and Media* (pp. 551–564). Routledge.

Arfah, Rizki. (2020). *Sanksi Tindak Pidana Hacking (Studi Analisis Undang-Undang ITE Dan Hukum Pidana Islam)*. Universitas Islam Negeri Sumatera Utara.

Balogun, Victor F., & Obe, Olumide O. (2010). E-crime in Nigeria: Trends, tricks, and treatment. *The Pacific Journal of Science and Technology*, *11*(1), 343–355.

Buchanan, Tom, & Whitty, Monica T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283.

Caroline, Evline, Kuntadi, Cris, & Pramukty, Rachmat. (2023). Pengaruh Pengalaman Auditor, Dukungan Manajemen Dan Efektivitas Pengendalian Internal Terhadap Efektivitas Fungsi Audit Internal. *Jurnal Economina*, *2*(6), 1487–1497.

Drew, Jacqueline M., & Farrell, Lucy. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537–549.

Edithya, Karina Veby. (2019). *Evaluasi Kinerja Polda Lampung Dalam Mewujudkan Pelayanan Prima Kepolisian Melalui Program E-Policing*.

Hasan, Muhammad, & Azis, Muhammad. (2018). *Pembangunan Ekonomi & Pemberdayaan Masyarakat: Strategi Pembangunan Manusia dalam Perspektif Ekonomi Lokal*. CV. Nur Lina Bekerjasama dengan Pustaka Taman Ilmu.

Pasaribu, Manerep, & Widjaja, Albert. (2022). *Manajemen Strategis di Era Kecerdasan Buatan*. Kepustakaan Populer Gramedia.

Simarmata, Janner, Iqbal, Muhammad, Hasibuan, Muhammad Said, Limbong, Tonni, & Albra, Wahyuddin. (2019). Hoaks dan media sosial: saring sebelum sharing. *Yayasan Kita Menulis*.

Soesanto, Edy, Purba, Lidia Margaretta, Aprilia, Bunga, Putra, Dwi Renaldy, & Putri, Sela Dwi. (2023). Implementasi Objek Vital, Pengamanan File dan Pengamanan Cyber di PT Pertamina. *IJM: Indonesian Journal of Multidisciplinary*, *1*(1), 96–105.

Suhaemin, Amin, & Muslih, Muslih. (2023). Karakteristik Cybercrime di Indonesia. *Edulaw: Journal of Islamic Law and Jurisprudance*, *5*(2), 15–26.

Suseno, Bayu. (2016). E-Polmas: Paradigma Baru Pemolisian Masyarakat Era Digital. *Jurnal Keamanan Nasional*, *2*(1), 77–110.

Sutarli, Ananta Fadli, & Kurniawan, Shelly. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, *3*(2), 4208–4221.

Wibowo, Arief, Wangsajaya, Yehu, & Surahmat, Asep. (2023). *Pemolisian Digital dengan Artificial Intelligence*. PT. RajaGrafindo Persada-Rajawali Pers.