JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455

**DOI:** https://doi.org/10.38035/jihhp.v6i4
https://creativecommons.org/licenses/by/4.0/
**Received**: 23 April 2026 | **Revised**: 19 Mei 2026 | **Accepted**: 24 Mei 2026

# Strategi Preventif Polda Jawa Barat dalam Menanggulangi Kejahatan *Phishing* pada Pemanfaatan Fitur *Buy Now Pay Later* (BNPL): Pendekatan Terintegrasi dan Peningkatan Efektivitas

**Ariq Fadhali Nasution[1], Riska Sri Handayani[2], Muhamad Erza Aminanto[3]**
[1]Universitas Indonesia, Jakarta Pusat, Indonesia, afadali619@gmail.com.
[2]Universitas Indonesia, Jakarta Pusat, Indonesia, riska.sri@ui.ac.id.
[3]Universitas Indonesia, Jakarta Pusat, Indonesia, Erza.aminanto@ui.ac.id.

Corresponding Author: afadali619@gmail.com[1]

***Abstract:*** *This research is motivated by the increasing trend of phishing crimes targeting Buy Now Pay Later (BNPL) services in West Java, which holds the highest number of Paylater users throughout 2025 to early 2026. This study aims to analyze the preventive strategy model of the West Java Regional Police (Polda Jawa Barat) and to formulate an integrated preventive strategy model involving law enforcement, the community, and BNPL service providers. The research employs a qualitative approach with field research methods, grounded in crime prevention theory and crime countermeasure theory. The findings indicate that the preventive strategies currently implemented by Polda Jawa Barat remain general in nature, encompassing primary prevention through digital literacy education, secondary prevention through cross-sector collaboration for early detection, and tertiary prevention through active cyber patrols conducted by the Cyber Crime Directorate of Polda Jawa Barat. The effectiveness of these strategies is assessed as low to moderate amid a continuously rising trend of cases. Therefore, this study recommends the development of an integrated preventive strategy model that combines proactive law enforcement, massive and sustainable digital literacy programs, and strategic collaboration with fintech service providers and relevant regulators such as OJK and BSSN, in order to strengthen early detection, reduce victim losses, and build digital security resilience among the people of West Java.*

***Keyword:*** *strategy, preventive, repressive, fintech, phishing*

**Abstrak:** Penelitian ini dilatarbelakangi oleh meningkatnya tren kejahatan *phishing* pada layanan *Buy Now Pay Later* (BNPL) di Jawa Barat sebagai provinsi dengan pengguna *Paylater* tertinggi sepanjang 2025 hingga awal 2026. Penelitian ini bertujuan menganalisis model strategi preventif Polda Jawa Barat serta merumuskan model strategi preventif terintegrasi antara penegak hukum, masyarakat, dan penyedia layanan BNPL. Penelitian menggunakan pendekatan kualitatif dengan metode penelitian lapangan, berlandaskan teori pencegahan kejahatan dan teori penanggulangan kejahatan. Hasil penelitian menunjukkan bahwa strategi

preventif yang diterapkan Polda Jawa Barat masih bersifat umum, mencakup pencegahan primer melalui edukasi literasi digital, pencegahan sekunder melalui kolaborasi lintas sektor untuk deteksi dini, serta pencegahan tersier melalui patroli siber aktif oleh Ditres Siber Polda Jabar. Efektivitas strategi tersebut dinilai masih rendah hingga sedang di tengah tren peningkatan kasus yang terus berlanjut. Oleh karena itu, penelitian ini merekomendasikan pengembangan model strategi preventif terintegrasi yang menggabungkan penegakan hukum proaktif, literasi digital yang masif dan berkelanjutan, serta kolaborasi strategis dengan penyedia layanan fintech dan regulator terkait seperti OJK dan BSSN, guna memperkuat deteksi dini, menekan kerugian korban, dan membangun ketahanan keamanan digital masyarakat Jawa Barat.

**Kata Kunci:** strategi, preventif, represif, *fintech*, *phishing*.

## PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah mengubah berbagai bidang kehidupan, mulai dari aspek sosial, ekonomi, hingga budaya. Namun, di samping manfaatnya, teknologi ini juga membawa risiko yang tidak kalah besar, tergantung pada cara pemanfaatannya oleh individu atau kelompok tertentu (Deb, 2014; Riskiyadi, 2020). Dampak positifnya sangat terasa karena memudahkan individu maupun kelompok dalam menjalankan aktivitas harian. Sebaliknya, dampak negatif muncul ketika teknologi disalahgunakan untuk melakukan kejahatan siber (*cybercrime*), yang pada akhirnya merugikan pihak lain (Gani, 2018).

Seiring dengan percepatan kemajuan teknologi, upaya penguatan sistem keamanan juga semakin digencarkan sebagai tanggapan atas lonjakan kasus *cybercrime* yang sangat tajam (Peters et al., 2018). Sayangnya, para pelaku *cybercrime* lebih cepat beradaptasi dan kreatif dalam menemukan cara-cara baru untuk menembus sistem keamanan yang telah dibangun oleh para ahli *cybersecurity*. Kondisi ini menjadi sangat mengkhawatirkan ketika pelaku kejahatan siber tersebut juga memiliki keahlian di bidang keamanan siber, sehingga metode terbarunya sulit dideteksi dan dicegah. Ketimpangan di mana serangan *cybercrime* terus berkembang dengan cepat sementara pertahanan *cybersecurity* cenderung tertinggal menjadi masalah krusial yang mendesak untuk segera diatasi (Corbet & Gurdgiev, 2017).

Perkembangan teknologi informasi dan komunikasi telah melahirkan berbagai inovasi, salah satunya adalah teknologi keuangan yang dikenal sebagai *fintech* (Lee & Jae, 2018; Sangwan et al., 2019). *Fintech* berkembang dalam berbagai layanan seperti pembayaran, transfer dana, remitansi, pinjaman (*lending*), *crowdfunding* atau urun dana, intermediasi keuangan, investasi ritel, perencanaan keuangan, riset keuangan, serta berbagai jasa keuangan lainnya (Das, 2019; Suryono et al., 2020). *Fintech* telah diterima secara luas oleh masyarakat karena kemampuannya untuk terus berkembang menjadi alat yang sangat efektif dan efisien dalam menyediakan layanan keuangan (Kou, 2019), sekaligus sesuai dengan pola hidup serta kebiasaan masyarakat modern (M. C. Shekar & Kumaran, 2019; Wang, 2021). Di sisi lain, kehadiran *fintech* juga menimbulkan ancaman serius terhadap kelangsungan lembaga keuangan konvensional seperti bank dan asuransi tradisional yang masih beroperasi secara manual (Broby, 2021; Şcheau, 2017). Perkembangan *fintech* terus menjadi perhatian utama di berbagai media (Zavolokina et al., 2016), disertai peningkatan penelitian yang sangat signifikan setiap tahun sejak kemunculannya (Kou, 2019).

Meskipun berkembang dengan sangat cepat, *fintech* tetap tidak terlepas dari berbagai risiko dalam penerapannya. Risiko yang dihadapi meliputi risiko teknologi dan risiko bisnis, yang variasinya bergantung pada karakteristik masing-masing platform *fintech* (Namchoochai et al., 2020; Suryono et al., 2020). Secara khusus, risiko finansial dan teknologi pada *fintech*

meliputi risiko diversifikasi, risiko yang ditransfer, risiko yang dikendalikan, serta risiko yang didanai (Rahmanto & Nasrulloh, 2019), dengan risiko teknologi menjadi tantangan paling besar. Risiko teknologi ini terutama berkaitan dengan keamanan data yang rentan terhadap serangan *cybercrime* (Singh & Rajput, 2019). Para pelaku *cybercrime* kerap memanfaatkan celah-celah dalam sistem *fintech* untuk melakukan penipuan, pemerasan, pencucian uang, serta berbagai jenis kejahatan lainnya yang melanggar hukum yang berlaku (Nikkel, 2020).

Secara umum, produk *fintech* berupa sistem yang dirancang secara khusus untuk menjalankan mekanisme transaksi keuangan tertentu. Salah satu inovasi yang paling populer adalah *fintech lending*, yang juga dikenal sebagai *fintech peer-to-peer* lending atau Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (LPMUBTI). Inovasi ini di bidang keuangan memanfaatkan teknologi untuk menghubungkan langsung antara pemberi pinjaman (*lender*) dan penerima pinjaman (*borrower*) tanpa memerlukan pertemuan tatap muka. Seluruh proses pinjam-meminjam dilakukan melalui platform yang disediakan oleh penyelenggara *fintech lending*, baik dalam bentuk aplikasi mobile maupun situs web (Otoritas Jasa Keuangan, n.d.). Menurut Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 Pasal 1 Ayat 3, Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang disebut *fintech* merupakan penyelenggaraan layanan jasa keuangan yang menghubungkan pemberi pinjaman dengan penerima pinjaman untuk melakukan perjanjian pinjam-meminjam dalam mata uang rupiah secara langsung melalui sistem elektronik berbasis internet.

Salah satu bentuk *fintech* yang sangat ramai digunakan oleh masyarakat Indonesia adalah *Paylater*. Skema alur penggunaan *Paylater* umumnya dimulai dari registrasi (pengisian data diri dan verifikasi), aktivasi, kemudian saat berbelanja memilih metode pembayaran *Paylater*, penyedia layanan akan membayar ke *merchant*, dan pengguna wajib melunasi tagihan sesuai tenor (cicilan atau bayar nanti) yang dipilih sebelum jatuh tempo untuk menghindari biaya denda serta dampak negatif terhadap skor kredit. Menurut data yang dirilis oleh Tempo.co tahun 2024 melalui laman webnya, diketahui demografi pengguna *Paylater* di Indonesia didominasi oleh generasi milenial dan generasi Z, dengan pengguna terbanyak tersebar di Provinsi Jawa Barat. Hal ini menjadi salah satu urgensi yang dilihat sebagai peneliti untuk kemudian diteliti lebih dalam.

Salah satu platform *e-commerce* terkemuka yang menerapkan metode *Paylater* adalah Platform X, melalui fitur BNPL (Lesilolo et al., 2024). Menurut laporan keuangan Platform X pada kuartal keempat tahun 2021, platform ini mencatatkan total 1,3 miliar transaksi serta 136,4 juta pengguna aktif bulanan di seluruh wilayah operasinya, termasuk Asia Tenggara dan Taiwan. Pada kuartal kedua tahun 2022, berdasarkan data *Iprice* (2022), Platform X menduduki posisi kedua sebagai situs dengan jumlah pengunjung terbanyak di Indonesia, mencapai 131.296.667 pengunjung (Lesilolo et al., 2024). Untuk layanan BNPL sendiri, Platform X bekerja sama dengan PT Lentera Dana Nusantara (LDN), sebuah perusahaan *peer-to-peer lending* yang terdaftar dan diawasi oleh OJK. Pengguna aplikasi Platform X dapat memanfaatkan SPaylater sebagai solusi pembayaran cicilan tanpa kartu kredit dan tanpa jaminan, memungkinkan belanja sekarang dan bayar nanti dengan cara yang lebih fleksibel.

Hingga saat ini, popularitas BNPL terus meningkat pesat di Indonesia. Berdasarkan berbagai sumber terkini, layanan ini menjadi salah satu *Paylater* paling banyak digunakan, terutama oleh Gen Z dan milenial, berkat integrasi langsung dengan ekosistem Platform X yang menawarkan promo menarik, kemudahan akses, serta limit yang kompetitif (hingga Rp15 juta atau lebih bagi pengguna aktif). Kolaborasi dengan PT Lentera Dana Nusantara tetap berjalan, dengan layanan seperti SPinjam juga tersedia sebagai opsi pinjaman tunai tambahan. Fenomena ini mencerminkan bagaimana *fintech Paylater* telah menjadi bagian integral dari gaya hidup belanja digital masyarakat Indonesia. Menurut DSResearch (2020), 54,3% masyarakat Indonesia menggunakan SPaylater, diikuti oleh GoPay Paylater (50,5%), OVO Paylater (28,9%), dan sebagainya (Lesilolo et al., 2024).

Tingginya jumlah pengguna *Paylater* di Indonesia mencerminkan bahwa layanan keuangan digital yang mudah diakses memberikan dampak positif terhadap inklusi keuangan. Namun, kemajuan ini juga disertai dengan peningkatan risiko kejahatan siber, terutama *phishing* yang menargetkan data sensitif serta aset finansial pengguna *fintech*. Selama lima tahun terakhir, Indonesia mengalami lonjakan berbagai bentuk kejahatan siber yang menyasar sektor keuangan secara masif.

Salah satu bentuk kejahatan yang paling umum adalah penipuan perbankan online, di mana para pelaku memanfaatkan teknik canggih seperti *phishing*, *malware*, dan rekayasa sosial untuk memperoleh akses tidak sah ke rekening bank individu (Erdiyanto, 2023). Sejalan dengan itu, kasus penipuan pembayaran *mobile* juga terus meningkat dalam beberapa tahun belakangan, dengan pelaku menggunakan taktik seperti penukaran kartu SIM, aplikasi mobile palsu, serta transaksi tidak sah (Buana, 2022). Sementara itu, popularitas mata uang kripto di Indonesia turut menarik perhatian para penjahat yang mengeksploitasi investor yang kurang berpengalaman melalui skema ponzi, *initial coin offering* (ICO) palsu, serta penipuan investasi kripto. Otoritas Jasa Keuangan (OJK) bahkan telah memperingatkan masyarakat mengenai risiko investasi kripto yang tidak teregulasi (Atmojo & Fuad, 2023).

Di sisi lain, pencurian data dan *phishing* identitas menjadi masalah yang terus berulang di Indonesia. Penjahat siber secara aktif menargetkan *database* informasi pribadi dari bank, platform *e-commerce*, serta lembaga pemerintah guna memperoleh data sensitif, sehingga menyebabkan peningkatan kasus pencurian identitas yang mengkhawatirkan. Badan Siber dan Sandi Negara (BSSN) melaporkan peningkatan signifikan insiden pembobolan data dalam beberapa tahun terakhir (Kusuma & Rahmani, 2022). Lebih jauh lagi, kejahatan keuangan digital juga dikaitkan dengan aktivitas pencucian uang serta pendanaan terorisme, di mana para pelaku memanfaatkan platform *online* untuk mentransfer dana ilegal sehingga menyulitkan aparat dalam mendeteksi dan mencegah aktivitas tersebut.

Dari berbagai kasus kejahatan siber yang berhasil dikumpulkan oleh peneliti, terlihat bahwa kejahatan siber khususnya di bidang keuangan harus ditangani secara serius dan segera. Hal ini didukung oleh data dari Otoritas Jasa Keuangan (OJK), yang menemukan lebih dari 340 tautan *impersonation* yang meniru identitas lembaga keuangan resmi. Berdasarkan data OJK melalui Indonesia *Anti-Scam Center* (IASC), diketahui data kasus penipuan daring yang terjadi selama 2024 hingga bulan Oktober 2025, dapat diamati pada tabel berikut ini:

**Tabel 1. Data Kasus Penipuan Daring Tahun 2024-Oktober 2025**

| No | Jenis Kasus | Jumlah Kasus | Kerugian (Rp) | Keterangan |
|---|---|---|---|---|
| 1 | Penipuan belanja daring | 53.928 | 988 miliar | - |
| 2 | *Fake call* (penipuan mengatasnamakan pihak lain) | 31.298 | 1.31 triliun | - |
| 3 | Penipuan investasi | 19.850 | 1,09 triliun | - |
| 4 | Total laporan melalui IASC (hingga pertengahan Oktober 2025) | > 299.000 | Triliunan rupiah | Sekitar 299.273 laporan hingga 16 Oktober 2025 dengan kerugian mencapai Rp7 triliun |
| 5 | Aduan konsumen melalui Aplikasi Portal Perlindungan Konsumen (APPK) | 43.101 | - | Hingga Oktober 2025; sektor *fintech* dan perbankan paling banyak dikeluhkan |

Sumber: OJK, 2025

UU ITE mengklasifikasikan kejahatan siber menjadi dua kelompok. Kelompok pertama meliputi kejahatan yang secara langsung menargetkan internet, komputer, atau teknologi terkait lainnya, yang merupakan jenis kejahatan baru seiring perkembangan teknologi. Kelompok kedua berkaitan dengan isi atau konten yang melanggar hukum, disebut konten ilegal, yang sebenarnya merupakan tindak pidana konvensional yang telah diatur sebelumnya, tetapi dilakukan dengan memanfaatkan sarana elektronik (Agung et al., 2022). Contoh nyata

dari kelompok kedua adalah pencurian data pribadi yang dikombinasikan dengan penipuan, khususnya terhadap nasabah bank. Pelaku biasanya menggunakan teknik *phishing*, yaitu dengan memancing korban untuk secara sukarela menyerahkan data pribadinya. Caranya, pelaku mengaku sebagai pihak resmi seperti bank atau lembaga terpercaya. Akibatnya, korban tidak sadar data tersebut dieksploitasi untuk kejahatan, sementara bank yang namanya disalahgunakan mengalami kerugian reputasi yang serius.

*Phishing* didefinisikan sebagai upaya memperoleh informasi penting seperti nama akun, kata sandi, dan data finansial (nomor kartu, PIN, OTP) dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik, melalui tautan atau situs web palsu yang meniru entitas resmi (Hanifah, 2023; Nervia et al., 2025). Modus operandi pelaku semakin kompleks, termasuk penggunaan situs palsu, manipulasi psikologis, hingga teknik *fake BTS* (Base Transceiver Station) untuk mengirim pesan palsu (Oktaviana & Rinaldi, 2025). Sejalan dengan pemahaman tersebut, definisi lainnya menyatakan bahwa tindakan *phishing* itu sendiri dianggap sebagai bentuk penipuan di mana pelaku mencoba memperoleh informasi pribadi dengan maksud menipu korban. Perlindungan hukum menjadi krusial untuk menciptakan lingkungan digital yang lebih aman dan untuk memberikan insentif bagi upaya perlindungan keamanan siber secara menyeluruh. Dalam hal ini, hukuman pidana tidak hanya bertujuan memberi efek jera kepada pelaku, tapi juga menjadi peringatan bagi masyarakat agar tidak melakukan tindak kejahatan yang sama, sekaligus mengajak semua orang untuk lebih waspada dan berhati-hati dalam bertindak (Diniyah, 2022).

*Phishing* yang terjadi di Indonesia tidak luput menyerang para pengguna SPL. Dicatat oleh sejumlah media dan lembaga publikasi lainnya, dinyatakan bahwa Otoritas Jasa Keuangan (OJK) merilis laporan bahwa kerugian akibat penipuan keuangan (*scam*) sebesar Rp 700 miliar tercatat sejak November 2024 hingga Februari 2025 (Money Kompas.co, 2025). Data ini sesuai dengan laporan resmi OJK melalui Indonesia *Anti-Scam Centre* (IASC), di mana total kerugian masyarakat yang dilaporkan mencapai Rp700,2 miliar sejak 22 November 2024 hingga 9 Februari 2025, dengan sebagian dana berhasil diblokir sekitar Rp106-107 miliar. Hal ini diperkuat oleh tren kasus *phishing* yang fluktuatif namun tetap tinggi, di mana data dari berbagai sumber seperti IDADX (Indonesia *Anti-Phishing* Data *Exchange*) menunjukkan peningkatan pada periode sebelumnya (misalnya, 26.675 laporan pada Q1 2023 saja, dengan tren naik dari tahun-tahun sebelumnya), dan BSSN serta OJK mencatat lonjakan insiden siber termasuk *phishing* yang terus berlanjut hingga 2025, meskipun tidak ada angka bulanan spesifik di bawah 2000 kasus per bulan secara konsisten dari sumber tersebut.

Dalam penelitian yang dilakukan oleh Puspitasari dan Sutabri (2023), salah satu kasus *phishing* yang dibahas terjadi pada tahun 2021. Saat itu, seorang pelaku berpura-pura sebagai penjual dan mengirim pesan singkat kepada korban terkait pesanan mereka. Pelaku mengklaim bahwa layanan pengiriman yang dipilih sedang bermasalah, lalu meminta korban untuk mengganti opsi pengiriman melalui tautan yang dikirimkannya. Korban pun mengikuti instruksi, mengisi semua data yang diminta (termasuk PIN Platform XPay miliknya) tanpa sadar bahwa tautan tersebut sebenarnya adalah link *phishing* yang dibuat untuk mencuri informasi pribadi. Saat itu pelaku masuk ke akun Platform X pengguna dan memiliki pinjaman Platform X (SPL) senilai Rp 3 juta. Pengguna segera menghubungi *Customer Service* (CS) Platform X dan tidak butuh waktu lama bagi pihak *e-commerce* terkait untuk menyelesaikan masalah tersebut. Hal ini kembali menjadi salah satu pertimbangan peneliti untuk melakukan penelitian lanjutan terkait penanggulangan terhadap kasus tindak pidana *phishing* yang dilakukan khususnya pada pengguna BNPL di wilayah hukum Polda Jawa Barat.

Pemerintah Indonesia telah berupaya merespons ancaman *cybercrime* ini melalui kerangka regulasi. Kejahatan *phishing* tercantum dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah oleh UU Nomor 19 Tahun 2016, khususnya Pasal 28 ayat (1) dan Pasal 35 yang berkaitan dengan

penyebaran berita bohong yang merugikan konsumen dan manipulasi informasi elektronik (Az-zahra & Labib, 2024; Hanifah, 2023). Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) semakin memperkuat aspek perlindungan data korban (Az-zahra & Labib, 2024; Maramis, 2025). Di sektor keuangan, Peraturan Otoritas Jasa Keuangan (POJK) juga mewajibkan penyedia layanan digital untuk menerapkan manajemen risiko dan perlindungan konsumen yang komprehensif (Az-zahra & Labib, 2024). Namun, regulasi yang bersifat umum ini terkadang belum maksimal dalam diterapkan pada sektor fintech yang sangat dinamis (Riskiyadi et al., 2021).

Pengesahan dan implementasi Undang-Undang ITE awalnya dilakukan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selanjutnya, Undang-Undang ini mengalami revisi dan perubahan kedua melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berlaku hingga saat ini. Kejahatan siber dalam bentuk *phishing* di Indonesia saat ini dimungkinkan dapat dikenakan Pasal 35, karena *phishing* via pembuatan situs palsu yang meniru situs asli yang resmi. Selain itu, *cybercrime phishing* juga dikenakan Pasal 28 ayat (1), karena *phishing* melibatkan tindakan penipuan untuk menyesatkan orang lain. Dalam hal ini, *phishing* mengarahkan individu yang tertipu untuk mengakses suatu tautan yang menuju ke web palsu, lalu memberikan perintah palsu untuk memperbarui informasi pribadi rahasia ke dalam situs palsu yang dibuat oleh pelaku *phishing*. Akibatnya, informasi pribadi rahasia tersebut terungkap kepada pelaku *phishing* dan menyebabkan kerugian pada korban (Gulo et al., 2020).

Dengan adanya regulasi tersebut serta perbandingan penanggulangan *phishing* di beberapa negara tetangga, hal ini tentu menjadi dasar bagi Polri untuk melakukan upaya penegakan hukum sebagai bentuk penanggulangan dan pencegahan tindak pidana *phishing*, sehingga dapat meminimalisir kerugian yang dialami masyarakat. Pidana tidak hanya berfungsi sebagai penghukuman terhadap pelaku, tetapi juga sebagai instrumen untuk mewujudkan kepastian hukum dan keadilan, yang harus dipertanggungjawabkan secara penuh.

Sesuai dengan latar belakang masalah yang telah diuraikan termasuk data-data serta penjelasan sederhana mengenai tindak pidana *phishing* serta alasan mengapa *phishing* pada BNPL menjadi hal yang cukup mengkhawatirkan masyarakat, khususnya di wilayah hukum Polda Jawa Barat mengingat jumlah pengguna akun *Paylater* di provinsi tersebut cukup tinggi. Urgensi utama penelitian ini terletak pada fakta bahwa tindak pidana *phishing* khususnya pada BNPL tidak hanya menimbulkan kerugian finansial signifikan bagi individu dan merusak kepercayaan masyarakat terhadap sistem keuangan digital secara keseluruhan, tetapi juga mengancam keamanan data pribadi secara masif. Bahkan, tercatat adanya kasus kebocoran data pribadi warga Jawa Barat, seperti klaim *hacke*r "*DigitalGhostt*" pada Juli 2025 yang menyebutkan penguasaan data pribadi sekitar 4,6 juta warga Jawa Barat, serta penangkapan sindikat kejahatan siber oleh Polda Jabar yang melibatkan modus phishing.

Meskipun kasus penangkapan sindikat phishing spesifik pada BNPL di Jawa Barat tidak banyak terdokumentasi secara publik dalam periode terkini, terdapat kasus penipuan terkait *Paylater* (seperti dugaan penipuan berkedok titip limit *Paylater* di Ciamis yang ditangani Polres Ciamis dengan koordinasi tim siber Polda Jabar pada 2025), serta kasus serupa di wilayah lain yang menunjukkan pola lintas provinsi dengan kerugian mencapai miliaran rupiah (misalnya modus penipuan BNPL di Jambi dengan kerugian Rp4,5 miliar pada 2025). Data ini menegaskan bahwa permasalahan *phishing fintech* merupakan ancaman nyata dan mendesak di wilayah hukum Polda Jawa Barat, terutama mengingat Jawa Barat secara konsisten menduduki posisi teratas sebagai provinsi dengan pengguna *Paylater* terbanyak di Indonesia (sekitar 27-34,5% dari total nasional berdasarkan data Pefindo Biro Kredit/IdScore hingga 2024-2025, dengan total debitur nasional mencapai lebih dari 16 juta).

Maraknya kejahatan *phishing* pada layanan *fintech Paylater*, termasuk SPL, telah menjadi ancaman serius bagi keamanan digital masyarakat Indonesia, khususnya di Jawa Barat sebagai provinsi dengan jumlah pengguna Paylater tertinggi. Data OJK melalui Indonesia *Anti-Scam Center* (IASC) menunjukkan lonjakan signifikan kasus penipuan daring, dengan ratusan ribu laporan dan kerugian mencapai triliunan rupiah sepanjang akhir 2024 hingga 2025, di mana sektor *fintech* dan perbankan mendominasi aduan konsumen. Kondisi ini tidak hanya menimbulkan kerugian finansial yang besar bagi masyarakat, tetapi juga melemahkan kepercayaan terhadap ekosistem keuangan digital yang tengah berkembang pesat.

Meskipun Polda Jawa Barat telah menerapkan strategi preventif berlapis melalui edukasi masyarakat, kolaborasi lintas sektor, serta patroli dan penindakan siber, pendekatan tersebut masih bersifat umum dan belum difokuskan secara khusus pada modus *phishing* berbasis *fintech Paylater*. Akibatnya, efektivitas strategi yang ada dinilai masih rendah hingga sedang di tengah tren peningkatan kasus yang terus terjadi. Kondisi ini mendorong urgensi pengembangan model strategi pencegahan yang lebih efektif dan terintegrasi oleh Polda Jawa Barat untuk menekan angka kejahatan *phishing* pada layanan SPL.

Berdasarkan latar belakang tersebut, penelitian ini merumuskan dua pertanyaan utama. Pertama, bagaimana model strategi preventif yang saat ini diterapkan oleh Polda Jawa Barat dalam menanggulangi kejahatan *phishing* pada layanan SPL, serta sejauh mana efektivitasnya dalam menekan angka kejahatan tersebut. Kedua, bagaimana pengembangan model strategi preventif terintegrasi yang lebih efektif dapat dirumuskan oleh Polda Jawa Barat melalui sinergi antara penegakan hukum, edukasi masyarakat, dan kolaborasi dengan penyedia layanan *fintech* SPL.

## METODE

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian lapangan. Penelitian ini berfokus pada analisis strategi preventif yang saat ini diterapkan oleh Polda Jawa Barat dalam menanggulangi kejahatan *phishing* pada layanan SPL, serta sejauh mana efektivitasnya dalam menekan angka kejahatan tersebut, dan pengembangan model strategi preventif terintegrasi yang lebih efektif dapat dirumuskan oleh Polda Jawa Barat melalui sinergi antara penegakan hukum, edukasi masyarakat, dan kolaborasi dengan penyedia layanan *fintech* (SPL). Pengumpulan data dilakukan melalui wawancara kepada narasumber penelitian yang telah ditentukan, pengamatan dan studi dokumen, lalu hasil penelitian ini dilakukan uji validitas-reliabilitas, reduksi data, serta sajian dan verifikasi data.

## HASIL DAN PEMBAHASAN

### Model Strategi Preventif Polda Jawa Barat Dalam Menanggulangi Kejahatan *Phishing* Pada Layanan SPL, dan Sejauh Mana Efektivitasnya Dalam Menekan Angka Kejahatan

Model strategi preventif yang saat ini diterapkan oleh Polda Jawa Barat dalam menanggulangi kejahatan *phishing* pada layanan BNPL masih bersifat umum dan terintegrasi dalam penanganan kejahatan siber, karena kasus *phishing* spesifik pada BNPL tidak banyak terdokumentasi secara publik sebagai program khusus terpisah. Namun, berdasarkan praktik yang ada, strategi preventif Polda Jawa Barat mengikuti pendekatan Polri secara nasional dengan penekanan pada pencegahan (preventif), edukasi masyarakat, kolaborasi lintas sektor, dan pemantauan siber.

Perlu diketahui bahwa model strategi preventif Polda Jawa Barat dalam menanggulangi kejahatan siber, dirancang secara *multilayer* (bertingkat). Pendekatan ini mengadopsi konsep pencegahan kriminalitas yang umum digunakan oleh Polri secara nasional, di mana upaya dibagi menjadi tiga tingkatan yaitu primer, sekunder, dan tersier. Tujuannya adalah mengurangi risiko kejahatan sebelum terjadi (primer), mendeteksi dan menghentikan ancaman

dini (sekunder), serta menangani dampak setelah kejadian untuk mencegah pengulangan (tersier) (Nurlaela, 2020).

Preventif primer berupa edukasi dan kesadaran masyarakat (sosialisasi offline/online), dimana tingkatan ini fokus pada pencegahan sebelum kejahatan terjadi, dengan cara meningkatkan kesadaran dan literasi digital masyarakat agar tidak mudah menjadi korban. Strategi ini bersifat proaktif dan jangka panjang, karena menargetkan akar masalah seperti kurangnya pengetahuan tentang modus phishing, misalnya, link palsu, OTP palsu, atau tawaran limit *Paylater* fiktif. Preventif primer ini tujuannya yaitu agar masyarakat, khususnya pengguna *Paylater* di Jawa Barat yang mendominasi nasional, lebih waspada terhadap modus penipuan yang memanfaatkan platform seperti SPL. Contohnya, Polda Jabar melakukan sosialisasi dan edukasi di sekolah, kampus, serta masyarakat umum tentang privasi digital, etika online, dan bahaya *phishing*. Pada November 2025, mendorong pendidikan privasi digital di sekolah untuk menekan pelanggaran siber seperti penipuan digital dan doxing, webinar dan diskusi bersama Diskominfo Jabar, seperti webinar Sandikamimania Series #64 pada November 2025 tentang strategi pertahanan siber *anti-scam* dan *anti-phishing*, kampanye melalui media sosial (Instagram @ccic.jabar) dan imbauan langsung, termasuk pelatihan internal dan eksternal tentang *malware/phishing* misalnya, kerja sama dengan Inixindo Bandung pada September 2025.

Kemudian preventif sekunder, berupa kolaborasi dengan stakeholder untuk deteksi dini dan blokir ancaman. Tingkatan ini menargetkan deteksi dini dan intervensi cepat terhadap ancaman yang sudah muncul, sebelum merugikan korban secara luas. Fokus pada kerja sama lintas sektor untuk mengidentifikasi, memblokir, dan menghentikan serangan *phishing*. Tujuannya yaitu untuk mengurangi volume ancaman sebelum mencapai korban, terutama di provinsi dengan pengguna *Paylater* tertinggi seperti Jawa Barat. Contoh penerapan oleh Polda Jabar yaitu kerja sama dengan platform keuangan digital (*fintech*) untuk mencegah kejahatan siber di sektor finansial, seperti kolaborasi dengan Akulaku pada 2022 untuk perlindungan nasabah dari *phishing* dimana pendekatan serupa masih berlanjut hingga 2025, koordinasi dengan OJK, BSSN, dan lembaga lain untuk berbagi informasi ancaman, pemblokiran situs palsu, serta deteksi dini modus *phishing* yang menyasar *fintech*, dan kolaborasi dengan Bareskrim Polri dan instansi terkait untuk patroli siber bersama, termasuk *take down* konten penipuan seperti *link phishing* yang meniru Platform X.

Kemudian preventif tersier, berupa pemantauan siber aktif via Ditres siber dan respons cepat terhadap laporan. Tingkatan ini bersifat responsif setelah kejahatan terjadi, dengan tujuan meminimalkan dampak, memberikan efek jera, dan mencegah pengulangan. Ini meliputi pemantauan aktif dan penanganan cepat laporan masyarakat. Tujuannya adalah untuk mengurangi kerugian korban dan memperkuat sistem pencegahan secara keseluruhan. Contoh penerapan oleh Polda Jabar yaitu Ditres Siber Polda Jabar aktif melakukan patroli siber, deteksi ancaman, dan respons terhadap laporan masyarakat (melalui kanal resmi seperti 110 atau aplikasi Patroli Siber), penindakan sindikat *phishing* dan penipuan digital, termasuk koordinasi dengan tim siber untuk kasus terkait *Paylater*, meski kasus spesifik BNPL jarang dipublikasikan terpisah dan efek jera melalui penangkapan dan pengungkapan kasus, yang juga membantu meningkatkan kepercayaan masyarakat untuk melapor lebih awal.

Polda Jawa Barat memiliki Direktorat Reserse Siber (Ditres Siber) yang resmi dibentuk sejak sekitar 2024 (di bawah Ditreskrimsus sebelumnya), yang menjadi unit menangani kejahatan siber termasuk *phishing*. Strategi preventifnya meliputi:

Edukasi dan Sosialisasi Masyarakat

Polda Jabar aktif melakukan diskusi strategis, sosialisasi, dan kampanye bersama instansi terkait seperti Dinas Komunikasi dan Informatika (Diskominfo) kota/kabupaten. Contohnya, pada September 2025, Diskominfo Kota Bandung bersama Unit Penanganan Siber Polda Jabar menggelar diskusi untuk antisipasi *phishing* dan memperkuat keamanan siber warga.

Komitmen ini meliputi langkah preventif seperti edukasi tentang modus *phishing* misalnya, link palsu, OTP palsu, atau tawaran *cashback* palsu pada platform seperti BNPL untuk meningkatkan kesadaran masyarakat, terutama pengguna *fintech* di Jawa Barat yang mendominasi pengguna *Paylater* nasional.

Kolaborasi dengan Platform dan Lembaga Keuangan

Polda Jabar pernah menggandeng platform keuangan digital (contoh: PT Akulaku pada 2022) untuk mencegah *phishing* di sektor finansial, termasuk komitmen meningkatkan keamanan dan perlindungan dari risiko *phishing*. Meskipun tidak spesifik SPL, pendekatan serupa berlaku untuk *fintech* lain, termasuk kolaborasi dengan OJK, BSSN, dan platform e-commerce untuk berbagi informasi ancaman, pemblokiran tautan palsu, serta edukasi pengguna. Platform X sendiri mendorong pelaporan ke Pusat Bantuan atau OJK, yang selaras dengan upaya Polri.

Patroli dan Pemantauan Siber

Melalui Ditres Siber, Polda Jabar melakukan pemantauan akun/aktivitas siber yang berpotensi *phishing*, hoaks, atau penipuan *fintech*, termasuk deteksi dini situs palsu yang meniru Platform X atau meminta data sensitif (seperti OTP untuk aktivasi Paylater). Patroli siber ini juga meliputi respons cepat terhadap laporan masyarakat via kanal resmi Polri.

Penindakan dan Pencegahan Represif

Meskipun fokus preventif, pencegahan juga didukung penindakan sindikat *phishing*, contoh kasus serupa di wilayah lain seperti Jambi atau Jatim menunjukkan pola lintas provinsi. Di Jawa Barat, ada penangkapan sindikat siber (termasuk phishing umum), dan koordinasi dengan tim siber untuk kasus terkait *Paylater*. Pencegahan melalui efek jera dari penegakan hukum berdasarkan UU ITE dan UU PDP (Iman dan khoirul, 2025).

Adapun efektivitas strategi preventif yang diterapkan oleh Polda Jawa Barat dalam menekan angka kejahatan *phishing*, khususnya pada layanan SPL, masih terbatas dan belum optimal berdasarkan tren data terkini hingga awal 2026. Meskipun ada upaya edukasi, kolaborasi, dan penindakan melalui Ditres Siber, angka kasus *phishing* serta penipuan *fintech* secara nasional, termasuk di Jawa Barat sebagai provinsi dengan pengguna *Paylater* tertinggi, terus menunjukkan peningkatan signifikan daripada penurunan.

Lonjakan Kasus Kejahatan Siber Secara Umum di Jawa Barat

Sepanjang 2025, Polda Jabar mencatat 156 perkara kejahatan siber, naik lebih dari dua kali lipat dibandingkan tahun sebelumnya. Hal ini menunjukkan bahwa meskipun ada pencegahan melalui sosialisasi dan patroli siber, ancaman *phishing* serta penipuan online termasuk yang menyasar *fintech* seperti *Paylater*, masih mendominasi dan belum terkendali secara efektif. Polda Jabar sendiri menekankan pentingnya literasi digital, tapi pencegahan belum berjalan seimbang dengan penindakan.

Tren Nasional *Phishing* dan Penipuan *Fintech*

*Phishing* di Indonesia terus meningkat sepanjang 2025–2026, dengan teknik semakin canggih, misalnya *deepfake*, *vishing*, APK palsu, dan *social engineering*. Data BSSN dan OJK menunjukkan lonjakan insiden siber secara keseluruhan, dengan kerugian akibat penipuan *online* mencapai lebih dari Rp2,6 triliun hingga Mei 2025, dan laporan harian penipuan digital di Indonesia jauh lebih tinggi (3–4 kali) dibanding negara lain. Kasus spesifik *Paylater* (termasuk SPL) melibatkan modus seperti permintaan OTP palsu, tawaran limit tambah, *cashback* fiktif, atau gestun (pencairan tunai) yang dimanfaatkan penipu. Modus ini marak dilaporkan sepanjang 2025, dengan kerugian individu mencapai puluhan juta hingga miliaran rupiah dengan contoh kasus di Jambi Rp4,5 miliar via BNPL pada 2025. Di Jawa Barat, sebagai daerah dengan pengguna *Paylater* terbanyak (27–34,5% nasional), pola serupa kemungkinan besar terjadi meski tidak selalu terdokumentasi.

Upaya Penindakan dan Pencegahan

Polda Jabar aktif menangkap sindikat siber, misalnya kasus judi online lintas negara atau penipuan umum, tapi kasus *phishing* khusus BNPL jarang dipublikasikan secara terpisah. Penangkapan lebih banyak pada kasus terkait lain, sementara pencegahan bergantung pada edukasi bersama Diskominfo dan kolaborasi dengan OJK/IASC. Secara nasional, Polri menindak ribuan kasus manipulasi data elektronik (13.630 kasus hingga Oktober 2025), tapi ini lebih ke represif daripada preventif. Efek jera dari penangkapan ada, tapi tidak cukup menekan angka karena pelaku beradaptasi cepat.

Faktor Pembatas Efektivitas

Tren nasional menunjukkan ancaman siber naik 30% atau lebih, bahkan 200% dalam beberapa tahun terakhir menurut BSSN, dengan *phishing* sebagai modus favorit. Di Jawa Barat, meski ada penurunan pada kejahatan transnasional tertentu, kejahatan siber justru melonjak. Edukasi dan sosialisasi baik, tapi masyarakat, terutama Gen Z dan milenial pengguna *Paylater*, masih rentan karena literasi digital rendah dan modus penipu semakin halus dimana mereka tidak lagi hanya menggunakan link palsu, tapi pakai fitur resmi. Meski ada kerjasama dengan platform seperti Platform X, implementasi deteksi dini dan blokir ancaman belum sepenuhnya efektif mengurangi volume kasus (Barus dan Purba, 2025).

Jadi efektivitas strategi preventif Polda Jawa Barat masuk kategori rendah hingga sedang dalam menekan angka *phishing* pada SPL. Upaya preventif primer (edukasi) dan sekunder (kolaborasi) ada dan berkontribusi pada peningkatan kesadaran, tapi belum mampu membalik tren peningkatan kasus. Angka kejahatan siber di Jabar naik tajam pada 2025, dan tren nasional menunjukkan *phishing* tetap menjadi ancaman utama *fintech* tanpa tanda-tanda penurunan signifikan hingga 2026. Untuk hasil lebih baik, maka diperlukan penguatan kapasitas Ditres Siber, literasi digital masif, serta integrasi teknologi deteksi ancaman yang lebih advanced.

**Pengembangan Model Strategi Preventif Terintegrasi yang Lebih Efektif Oleh Polda Jawa Barat Melalui Sinergi Antara Penegakan Hukum, Edukasi Masyarakat, dan Kolaborasi Dengan Penyedia Layanan *Fintech* (SPL)**

Model strategi preventif terintegrasi dalam penanggulangan tindak pidana *phishing* pada pengguna BNPL oleh Polda Jawa Barat merupakan sebuah kerangka atau rancangan pendekatan yang komprehensif, terpadu, dan berlapis untuk mencegah kejahatan siber tersebut sebelum terjadi, bukan hanya menangani setelah kejadian (reaktif). Model ini bukan sekadar satu teknik tunggal, melainkan sistem strategi yang menggabungkan berbagai elemen secara sinergis agar saling memperkuat, sehingga lebih efektif daripada pendekatan parsial atau terpisah-pisah.

Di sisi lain, sinergi antara penegakan hukum, edukasi masyarakat, dan kolaborasi dengan penyedia layanan *fintech* (SPL) adalah pendekatan terpadu dan saling memperkuat di mana ketiga elemen ini bekerja secara bersamaan untuk mencegah dan menanggulangi tindak pidana *phishing* serta kejahatan siber terkait pada pengguna layanan seperti SPL. Sinergi ini bukan sekadar kerjasama biasa, melainkan integrasi strategis yang memanfaatkan kekuatan masing-masing pihak agar menciptakan efek pencegahan yang lebih besar daripada jika dilakukan secara terpisah. Pendekatan ini selaras dengan praktik nasional di Indonesia, di mana OJK, Polri, BSSN, dan industri *fintech* semakin memperkuat kolaborasi untuk melindungi masyarakat dari *scam* dan *cybercrime* di sektor keuangan digital (Maola, 2022).

Adapun pendekatan preventif menekankan pada upaya pencegahan primer dan sekunder (bukan hanya represif atau pemulihan), sehingga model ini bertujuan mengurangi kemungkinan korban terjebak *phishing* melalui kombinasi pencegahan teknis seperti peningkatan keamanan platform *fintech* dan pemantauan tautan palsu, pencegahan sosial seperti edukasi untuk mengubah perilaku pengguna agar lebih waspada, dan pencegahan institusional seperti penguatan regulasi, koordinasi lintas sektor, dan penegakan hukum proaktif.

Penegakan hukum sebagai elemen pertama fokus pada aspek represif dan preventif oleh aparat seperti Polda Jawa Barat, meliputi patroli siber aktif untuk mendeteksi situs *phishing* palsu yang meniru Platform X, pelacakan pelaku melalui analisis transaksi mencurigakan, penangkapan sindikat, misalnya modus *fake call* atau talangan limit *Paylater*, serta penerapan hukum seperti Pasal 28 ayat (1) dan Pasal 35 UU ITE serta UU PDP 2022. Sinergi di sini terwujud melalui koordinasi cepat dengan Indonesia *Anti-Scam Centre* (IASC) OJK, seperti yang diperkuat pada 2026 antara OJK dan Bareskrim Polri untuk mempercepat pemblokiran dana, pengembalian kerugian korban, dan penindakan hukum. Hasilnya, penegakan hukum tidak lagi reaktif saja, tapi proaktif dalam memutus rantai kejahatan sebelum merugikan lebih banyak pengguna.

Edukasi masyarakat sebagai elemen kedua men upaya jadi pencegahan primer yang menargetkan kerentanan pengguna, khususnya generasi milenial dan Gen Z di Jawa Barat yang mendominasi pengguna SPL. Edukasi ini meliputi kampanye literasi digital tentang pengenalan modus *phishing*, pesan palsu atas nama Platform X, permintaan OTP/PIN, *link update* data palsu, tips keamanan seperti verifikasi URL resmi, penggunaan 2FA, serta cara melapor ke kanal resmi seperti IASC, SIPELAKU OJK, atau *customer service* Platform X. Sinergi tercermin ketika Polda Jawa Barat berkolaborasi dengan OJK, Kominfo, sekolah, universitas, dan *influencer* untuk menyebarkan materi edukasi secara masif, baik offline (sosialisasi di kampus/pasar) maupun *online* (media sosial Polda dan kanal OJK). Kampanye seperti "Waspada *Phishing Paylater*" atau inisiatif nasional OJK seperti Kampanye Berantas *Scam*, menunjukkan bahwa edukasi menjadi lebih efektif ketika didukung oleh otoritas hukum dan regulator, sehingga meningkatkan kesadaran dan mengurangi tingkat korban.

Kolaborasi dengan penyedia layanan *fintech* (SPL) sebagai elemen ketiga melibatkan PT Lentera Dana Nusantara (LDN) selaku mitra Platform X, serta asosiasi seperti AFTECH. Kolaborasi ini meliputi berbagi intelijen ancaman seperti daftar URL *phishing*, pola transaksi fraud, pengembangan fitur keamanan bersama seperti alert transaksi mencurigakan, verifikasi biometrik tambahan, pembekuan akun sementara saat terdeteksi indikasi *phishing*, serta simulasi serangan bersama. Sinergi di sini diperkuat melalui MoU atau koordinasi dengan OJK dan BSSN seperti MoU AFTECH-BSSN 2025 untuk standar keamanan siber *fintech*, sehingga platform *fintech* tidak hanya mematuhi regulasi (POJK terkait BNPL/*Paylater*), tapi aktif berkontribusi dalam pencegahan. Contohnya, Platform X dapat langsung memblokir akun terkait *phishing* berdasarkan laporan Polri, sementara Polri mendapat data agregat untuk investigasi tanpa melanggar privasi.

Penegakan hukum akan mendapat dukungan data dari *fintech* untuk investigasi cepat, edukasi masyarakat diperkuat oleh kredibilitas Polri dan OJK serta contoh nyata dari kasus yang ditangani, kolaborasi *fintech* memastikan teknologi keamanan terus diperbarui berdasarkan masukan dari aparat hukum dan regulator. Hasil akhirnya adalah ekosistem yang lebih aman, di mana kerugian akibat *phishing* pada BNPL dapat ditekan, kepercayaan masyarakat terhadap *fintech* terjaga, dan inklusi keuangan digital berjalan tanpa ancaman berlebih.

Sesuai penjelasan tersebut, menurut kami pengembangan model strategi preventif terintegrasi oleh Polda Jawa Barat untuk menanggulangi tindak pidana *phishing* pada pengguna SPL, mutlak memerlukan pendekatan komprehensif yang menggabungkan tiga pilar yaitu penegakan hukum yang lebih responsif dan proaktif, edukasi masyarakat secara masif dan berkelanjutan, serta kolaborasi strategis dengan penyedia layanan *fintech* seperti BNPL melalui PT Lentera Dana Nusantara/LDN dan regulator terkait seperti Otoritas Jasa Keuangan (OJK) serta Badan Siber dan Sandi Negara (BSSN). Model ini dirancang untuk mengatasi ketimpangan antara kemajuan serangan *phishing* yang semakin canggih dan kapasitas pertahanan saat ini, terutama di Jawa Barat yang mendominasi pengguna *Paylater* nasional, yaitu sekitar 27-28% dari total debitur aktif, dengan lebih dari 16 juta debitur nasional per akhir

2024 hingga 2025 berdasarkan data Pefindo Biro Kredit/IdScore. Pendekatan terintegrasi ini bertumpu pada prinsip pencegahan berlapis (*layered defense*), di mana setiap pilar saling memperkuat untuk menciptakan ekosistem keamanan digital yang lebih tangguh.

Pilar pertama, penegakan hukum, harus ditingkatkan melalui pembentukan atau penguatan unit khusus di Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Jawa Barat, seperti subdirektorat siber yang fokus pada *phishing fintech*. Strategi preventif meliputi patroli siber intensif untuk memantau tautan palsu, situs impersonasi Platform X, dan kampanye *phishing* di media sosial serta aplikasi pesan. Polda Jawa Barat dapat mengadopsi model *co-location* dengan Indonesia *Anti-Scam Centre* (IASC) OJK, sebagaimana dilakukan secara nasional oleh Bareskrim Polri dan OJK pada 2026, untuk mempercepat identifikasi, pelacakan, dan pemblokiran dana/rekening pelaku. Penegakan represif juga diperkuat dengan penerapan Pasal 28 ayat (1) dan Pasal 35 UU ITE (sebagaimana diubah UU No. 1 Tahun 2024), ditambah sinergi dengan UU PDP No. 27 Tahun 2022 untuk perlindungan data korban. Efektivitasnya dapat diukur melalui peningkatan angka penangkapan sindikat *phishing* lintas provinsi, seperti kasus-kasus modus talangan limit *Paylater* atau *fake call* yang melibatkan SPL, serta pengembalian dana korban yang lebih cepat melalui koordinasi dengan IASC yang telah berhasil memblokir dan mengembalikan miliaran rupiah dalam kasus serupa.

Pilar kedua, edukasi masyarakat, menjadi kunci pencegahan primer mengingat demografi pengguna BNPL di Jawa Barat didominasi generasi milenial dan Gen Z yang rentan terhadap rekayasa sosial. Model ini mengusulkan program literasi digital berkelanjutan melalui kampanye "Waspada *Phishing Paylater*" yang digerakkan Polda Jawa Barat bekerja sama dengan Dinas Kominfo provinsi, sekolah/universitas, komunitas Gen Z, dan influencer lokal. Konten edukasi meliputi pengenalan modus *phishing* umum (seperti pesan palsu atas nama Platform X, permintaan OTP/PIN, atau link update data), tips verifikasi tautan resmi, aktivasi two-factor authentication (2FA), serta langkah pelaporan ke IASC/SIPELAKU OJK atau *call center* Platform X. Edukasi offline dapat dilakukan melalui sosialisasi di pasar tradisional, kampus, dan desa-desa dengan tingkat pengguna *Paylater* tinggi, sementara online melalui media sosial Polda Jabar dan kanal OJK. Pendekatan ini selaras dengan inisiatif nasional OJK seperti Kampanye Nasional Berantas *Scam*, yang menekankan literasi berkelanjutan untuk mengurangi korban *phishing* yang mencapai ratusan ribu laporan tahunan.

Pilar ketiga, kolaborasi dengan penyedia *fintech*, menjadikan model ini terintegrasi secara ekosistem. Polda Jawa Barat dapat menjalin MoU dengan SPL/LDN dan OJK Regional untuk berbagi intelijen ancaman (*threat intelligence*), seperti daftar IP/*phishing* URL mencurigakan, pola transaksi fraud, dan data agregat tanpa melanggar privasi (sesuai UU PDP). Kolaborasi ini meliputi pengembangan fitur keamanan bersama, seperti alert otomatis pada transaksi mencurigakan di aplikasi Platform X, verifikasi biometrik tambahan, dan mekanisme pembekuan sementara akun *Paylater* saat terdeteksi *phishing*. Sinergi dengan BSSN dan AFTECH seperti MoU 2025 untuk standar keamanan siber *fintech*, dapat diadopsi secara lokal, termasuk simulasi serangan *phishing* bersama dan pelatihan tim respons insiden Platform X. Kolaborasi ini juga melibatkan Satgas PASTI nasional untuk koordinasi lintas sektor, sehingga pencegahan tidak hanya reaktif tetapi proaktif dalam mendeteksi celah sistem *fintech* sebelum dieksploitasi (Leksi, Sahay dan Wulandari, 2025).

Model strategi preventif terintegrasi ini bersifat dinamis dan evaluatif, dengan indikator keberhasilan seperti penurunan laporan *phishing* terkait BNPL di Jawa Barat, minimal 20-30% dalam 1-2 tahun pertama, peningkatan tingkat pelaporan korban ke kanal resmi, serta pengurangan kerugian finansial masyarakat. Implementasinya memerlukan komitmen anggaran, pelatihan SDM, dan m*onitoring* berkala melalui *dashboard* bersama antar-pihak. Jadi, Polda Jawa Barat tidak hanya menanggulangi ancaman *phishing* saat ini, tetapi juga membangun ketahanan digital jangka panjang bagi masyarakat yang semakin bergantung pada *fintech* seperti SPL, sehingga mendukung inklusi keuangan tanpa mengorbankan keamanan.

## KESIMPULAN

Berdasarkan hasil penelitian, model strategi preventif Polda Jawa Barat dalam menanggulangi kejahatan *phishing* pada layanan *Buy Now Pay Later* (BNPL) telah menerapkan pendekatan *multilayer* yang mencakup pencegahan primer melalui edukasi dan sosialisasi literasi digital, pencegahan sekunder melalui kolaborasi lintas sektor untuk deteksi dini dan pemblokiran ancaman, serta pencegahan tersier melalui patroli siber aktif dan respons cepat oleh Ditres Siber Polda Jabar. Secara konseptual, strategi ini telah sejalan dengan kebijakan nasional Polri dan mampu meningkatkan kesadaran masyarakat serta memperkuat koordinasi antar instansi. Namun demikian, efektivitasnya dalam menekan angka kejahatan *phishing* pada layanan SPL masih tergolong rendah hingga sedang, sebagaimana tercermin dari meningkatnya tren kejahatan siber dan penipuan *fintech* di Jawa Barat sepanjang 2025 hingga awal 2026. Kondisi tersebut dipengaruhi oleh pesatnya adaptasi modus pelaku, tingginya jumlah pengguna *Paylater*, serta keterbatasan implementasi deteksi dini berbasis teknologi, sehingga upaya preventif yang telah berjalan belum mampu membalik tren peningkatan kasus secara signifikan.

Guna mengatasi keterbatasan tersebut, pengembangan model strategi preventif terintegrasi menjadi suatu keniscayaan yang mendesak. Model yang diusulkan merupakan pendekatan komprehensif dan berlapis yang menggabungkan sinergi penegakan hukum yang proaktif dan responsif, edukasi masyarakat yang masif serta berkelanjutan, serta kolaborasi strategis dengan penyedia layanan *fintech* dan regulator terkait seperti OJK dan BSSN. Model ini menempatkan pencegahan sebagai fokus utama melalui kombinasi aspek teknis, sosial, dan institusional, sehingga tidak sekadar bersifat reaktif terhadap kejahatan yang telah terjadi, melainkan mampu memutus rantai *phishing* sejak dini. Dengan dukungan patroli siber, berbagi intelijen ancaman, penguatan fitur keamanan *fintech*, serta peningkatan literasi digital khususnya bagi generasi milenial dan Gen Z, pendekatan terintegrasi ini diharapkan dapat menekan angka kejahatan dan kerugian akibat *phishing* secara signifikan, menjaga kepercayaan publik terhadap layanan SPL, serta membangun ekosistem keamanan digital yang tangguh dan berkelanjutan demi mendukung inklusi keuangan digital yang aman di Jawa Barat.

## REFERENSI


Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. PAMPAS: Journal of Criminal Law, 3(2), 212–222. https://doi.org/10.22437/PAMPAS.V3I2.23367

Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. PeerJ Computer Science, 10. https://doi.org/10.7717/PEERJ-CS.2487

Atmojo, R. N. P., & Fuad, F. (2023). Upaya Perlindungan Hukum Bagi Para Konsumen Pemegang Aset Kripto di Indonesia. Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat, 9(2), 254–276. https://doi.org/10.55809/TORA.V9I2.260

Az-zahra, I., & Labib, Z. M. (2024). Perlindungan Hukum Bagi Nasabah Dalam Kasus Phising Dan Siber Perbankan Di Indonesia. Yurisprudentia: Jurnal Hukum Ekonomi, 10(2), 405–425. https://doi.org/10.24952/YURISPRUDENTIA.V10I2.13952

Buana, S. E. W. (2022). Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending [Universitas Islam Indonesia]. https://dspace.uii.ac.id/bitstream/handle/123456789/39314/20912045.pdf?sequence=1&isAllowed=y

Cornelli, G., Gambacorta, L., & Pancotto, L. (2023). Buy now, pay later: a cross-country analysis. https://www.bis.org/publ/qtrpdf/r_qt2312e

Creswell, J. W. (2019). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Pustaka Pelajar.

Diniyah, K. J. (2022). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing. Dinamika, 28(5), 3756–3775. https://jim.unisma.ac.id/index.php/jdh/article/view/14600

Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. Jurnal InovasiGlobal,1(2), 71–79. https://doi.org/10.58344/JIG.V1I2.11

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 68–81. https://doi.org/10.22437/PAMPAS.V1I2.9574

Hanifah, L. (2023). Pengaturan Tindak Pidana Cyber Crime Dalam Bentuk Cyber Phishing Menurut Hukum Pidana Indonesia. Thesis, Universitas Islam Sultan Agung.

Iman, Muhammad Khoirul. (2025). Efektivitas Peran Kepolisian Dalam Penegakan Hukum Terhadap Jaringan Perjudian Online Berbasis Keadilan (Studi Kasus Direktorat Siber Polda Jawa Barat). Masters Thesis, Universitas Islam Sultan Agung.

Kavya, S., & Sumathi, D. (2025). Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection. Artificial Intelligence Review, 58(50), 1–46. https://doi.org/10.1007/S10462-024-11055-Z/TABLES/11

Khotimah, S. (2021). Implementasi Metode Role Playing Untuk Meningkatkan Motivasi Belajar Siswa Dalam Mata Pelajaran PPKN (Penelitian Tindakan Kelas X IPS 3 SMAN 15 Bandung).

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). SUPREMASI : Jurnal Hukum, 5(1), 46–63. https://doi.org/10.36441/SUPREMASI.V5I1.721

Kyaw, P. H., Gutierrez, J., & Ghobakhlou, A. (2024). A Systematic Review of Deep Learning Techniques for Phishing Email Detection. Electronics , 13(19), 3823. https://doi.org/10.3390/ELECTRONICS13193823

Lala Minhatul Maola. (2022). Peran Digital Forensik Dalam Mengungkap Tindak Pidana Cyber Crime (Studi Kasus Kepolisian Daerah Jawa Barat Tahun 2020). Skripsi, Uin Sunan Kalijaga Yogyakarta.

Leksi, L., Sahay, T., & Wulandari, V. P. (2025). The Legal Protection of Debtors as Victims of Personal Data Misuse in the Use of BNPL Service. Journal of Law, Politic and Humanities, 5(5), 4095–4101. https://doi.org/10.38035/jlph.v5i5.2008

Lesilolo, R. A. A., Kembau, A. S., & Malae, F. E. (2024). Menilai Pengaruh Manfaat, Kepercayaan, dan Kemudahan Terhadap Adopsi Layanan Paylater: Perspektif Pengguna BNPL di Jakarta. Jurnal Digismantech, 4(1). https://doi.org/10.30813/digismantech.v4i1.5956.g2952

Maramis, A. V. (2025). Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dalam Mengatasi Cybercrime Pada Kasus Phishing. Lex Privatum, 14(5). https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/60333

Moleong, L. J. (2021). Metodologi Penelitian Kualitatif (40th ed.). PT Remaja Rosdakarya.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 132, 103387. https://doi.org/10.1016/J.COSE.2023.103387

Nervia, C., Wardhana, K. A., Sie, P. A., Talim, T. L., & Hizkia, W. B. (2025). Analisis Yuridis Terhadap Kejahatan Phising Dalam Sistem Perbankan Digital Melalui Scam Link Berbahaya. Ikon –Jurnal Ilmiah Ilmu Komunikasi, 29(2), 13–30. https://doi.org/10.37817/IKON.V29I2.4739

Nurlaela, Siti (2020). Peran Dan Tanggung Jawab Kepolisian Negara Republik Indonesia Wilayah Jawa Barat Dalam Penegakan Hukum Tindak Pidana Siber Dikaitkan Dengan

Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Dan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Other thesis, Universitas Komputer Indonesia.

Oktaviana, H., & Rinaldi, K. (2025). Modus Operandi Phisher dalam Kejahatan Phishing (Studi Kasus Ditreskrimsus Polda Riau). Journal of Knowledge and Collaboration, 2(5), 655–658. https://doi.org/10.59613/XB36SV81

Otoritas Jasa Keuangan. (n.d.). FAQ Fintech OJK. Retrieved October 10, 2025, from https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/Documents/FAQ%20Fintech%20Lending.pdf

Puspitasari, D., & Sutabri, T. (2023). Analisis kejahatan phising pada sektor e-commerce di marketplace Platform X. Jurnal Digital Teknologi Informasi, 6(2). https://doi.org/10.32502/digital.v6i2.5653

Ramsi Meifati Barus, & Desborn Rico Purba. (2025). Analisis Risiko Cybercrime pada Layanan BNPL dan Implikasi terhadap Keamanan Data Pengguna. Al-Zayn : Jurnal Ilmu Sosial & Hukum, 3(6), 11523–11533. https://doi.org/10.61104/alz.v3i6.3594

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. Jurnal Manajemen Dan Organisasi, 12(3), 239–251. https://doi.org/10.29244/JMO.V12I3.33528

Sugeng, & Fitria, A. (2020). Aspek Hukum Digital Lending Di Indonesia. Jurnal Legislasi Indonesia, 17(4). https://finansial.bisnis.com/read/20190102/90/874715/ojk-pertumbuhan-kredit- 2018-1245.

Sugiyono. (2021a). Metode Penelitian Kuantitatif, Kualitatif, dan R&D (3rd ed.). ALFABETA.

Sugiyono. (2021b). Metode Penelitian Kuantitatif, Kualitatif, dan R&D (3rd ed.). ALFABETA.

Suzuki, Y. E., & Monroy, S. A. S. (2021). Prevention and mitigation measures against phishing emails: a sequential schema model. Security Journal, 35(4), 1162–1182. https://doi.org/10.1057/s41284-021-00318-x

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. Jurnal Impresi Indonesia, 2(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Tempo.co. (2024). Profil Pengguna Pay Later di Indonesia | tempo.co. Infografik Tempo. https://www.tempo.co/infografik/infografik/profil-pengguna-pay-later-di- indonesia-1184519

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. Jurnal Ilmu Hukum Jambi, 4(1), 43295. https://www.neliti.com/publications/43295/

Wiemken, M., Hildebrandt, K., Jeworutzki, A., & Putzar, L. (2025). Emotional Manipulation in Phishing Emails: Experimental Study of Affective Responses and Human Classification Errors in a Simulated Email Environment. Proceedings of the 18th ACM International Conference on PErvasive Technologies Related to Assistive Environments, PETRA 2025, 583–589. https://doi.org/10.1145/3733155.3736796