# Jurnal Kajian Hukum dan Sosial
Vol No.

Faculty of Law, Universitas Jenderal Soedirman, E-ISSN: 3124-3460
HR. Boenyamin 708, Purwokerto, Banyumas, Central Java, Indonesia.
jos.unsoed.ac.id/index.php/jkhs/index ✉ jkhs@unsoed.ac.id


# Analisis Kriminologis terhadap Komersialisasi Phishing Toolkit sebagai Bentuk Kejahatan Siber Terorganisasi


**Syahrul Diemas Nurjaman*, Danica Rosalia Heroesheinsa Meysha Risky Pratama, Ivan Ian Rama Putra, Muhammad Fariz Ilmi**

*Universitas Jenderal Soedirman*

**Corresponding Author: ✉ syahrul.nurjaman@mhs.unsoed.ac.id*



***Abstrak***

*informasi tidak hanya memfasilitasi efisiensi global, tetapi juga memicu proliferasi kejahatan siber melalui komersialisasi phishing toolkit. Penelitian ini bertujuan untuk menganalisis eksploitasi finansial global dan aktivitas penyamaran aset (cyber-laundering) dalam kasus distribusi piranti lunak ilegal "16Shop" berdasarkan Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb. Dari perspektif kriminologi dan hukum siber, penelitian ini mengkaji bagaimana keahlian teknologi informasi yang dimiliki pelaku disalahgunakan menjadi komoditas kriminal yang menimbulkan dampak destruktif lintas yurisdiksi.Metode penelitian yang digunakan adalah penelitian hukum normatif dengan mengombinasikan pendekatan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Sumber data utama berupa data sekunder yang bersumber dari bahan hukum primer, khususnya salinan putusan pengadilan terkait, serta bahan hukum sekunder seperti literatur kriminologi dan jurnal ilmiah. Analisis data dilakukan secara kualitatif-deduktif untuk membedah pertimbangan hukum majelis hakim dan pemenuhan unsur materiil tindak pidana. Hasil penelitian menunjukkan bahwa modus operandi pelaku melibatkan pengembangan script phishing yang menduplikasi platform digital global secara presisi, yang kemudian diperjualbelikan melalui transaksi mata uang kripto guna menyamarkan keuntungan ilegal sebesar Rp1,7 miliar. Majelis hakim menjatuhkan sanksi pidana berdasarkan dakwaan kombinasi Pasal 50 jo. Pasal 34 ayat (1) huruf a UU ITE dan Pasal 3 UU TPPU. Penelitian ini menyimpulkan bahwa penegakan hukum dalam kasus ini menunjukkan keberhasilan kolaborasi internasional, namun sanksi yang dijatuhkan masih memerlukan penguatan dari aspek deterensi kriminologis untuk menekan angka proliferasi alat kejahatan siber yang serupa di masa depan.*



***Kata Kunci***

*Phising; phising toolkit, pencucian uang, kriminologi siber, kejahatan siber.*

***Submitted**: 29 Mei 2026*
***Reviewed**: 15 Juli 2026*
***Accepted**: 06 Agustus 2026*

***Sitasi / How to Cite:***
*Nurjaman, Syahrul Diemas, Danica Rosalia Heroesheinsa Meysha Risky Pratama, Ivan Ian Rama Putra, dan Muhammad Fariz Ilmi. Analisis Kriminologis terhadap Komersialisasi Phishing Toolkit sebagai Bentuk Kejahatan Siber Terorganisasi. Jurnal Kajian Hukum dan Sosial, 3, no. 1, (2026): 70-87 10.20884/1.jkhs.2026.3.1. 10.20884/1.jkhs.2026.3.1.20861*


## PENDAHULUAN

Keamanan siber di era digital mengalami ancaman serius dari maraknya phising toolkit sebagai alat memfasilitasi kejahatan cyber di seluruh dunia. Phising toolkit merupakan perangkat lunak komprehensif yang dirancang khusus untuk menciptakan situs web palsu menyerupai platform terpercaya seperti PayPal, Amazon, dengan tingkat kemiripan visual yang hampir sempurna.[1]

[1] Rahmat Eka Putra R Palaloi. Rakhmadi Rahman, "ANALISIS DAN PENCEGAHAN SERANGAN SOSIAL ENGINERING PADA JARINGAN KOMPUTER STUDI KASUS PENIPUAN INVESTASI CRYPTO," *Jurnal Riset Sistem Informasi* 1, no. 3 (2024), https://doi.org/https://doi.org/10.69714/8b7xtv35.

Perkembangan toolkit ini memungkinkan pelaku menyebarkan email phishing massal ke korban global, mencuri data sensitif seperti kredensial login, informasi kartu kredit, dan detail pribadi lainnya yang kemudian dimanfaatkan untuk transaksi ilegal.[2] Di Indonesia, kasus semacam ini meningkat tajam seiring kemajuan teknologi informasi, menyebabkan kerugian finansial mencapai miliaran rupiah serta erosi kepercayaan publik terhadap transaksi elektronik dan layanan digital.[3]

Ancaman ini tidak hanya merugikan individu secara pribadi tetapi juga melemahkan stabilitas ekonomi nasional melalui potensi pencucian uang hasil kejahatan siber yang sulit dilacak. Selain itu, distribusi toolkit mempercepat proliferasi kejahatan terorganisir lintas negara.[4] Oleh karena itu, penegakan hukum terhadap distribusi phishing toolkit menjadi prioritas utama dalam strategi nasional keamanan siber.

Phishing toolkit telah menjadi fenomena sosial yang meresahkan masyarakat modern dengan korban mencapai jutaan secara global setiap tahunnya akibat penyebaran masif melalui email dan media sosial. Laporan internasional menunjukkan peningkatan penggunaan toolkit ini oleh kelompok kriminal terorganisir untuk menargetkan pengguna platform keuangan digital, termasuk konversi hasil curian ke cryptocurrency.[5] Di Indonesia, survei menunjukkan ribuan kasus penipuan online terkait phishing setiap tahun, menyebabkan kerugian finansial miliaran rupiah serta trauma psikologis berkepanjangan bagi korban dari berbagai lapisan masyarakat. Fakta ini diperburuk oleh rendahnya literasi siber di kalangan masyarakat, khususnya generasi muda yang rentan terhadap jebakan email palsu berbahasa lokal atau internasional.[6] Selain itu, pola transaksi cryptocurrency dari hasil phishing semakin menyulitkan pelacakan aset ilegal oleh aparat penegak hukum. Dampak sosialnya mencakup hilangnya kepercayaan terhadap e-commerce, peningkatan kemiskinan akibat pencurian data finansial, dan beban psikologis kolektif.[7] Fakta sosial ini menggarisbawahi urgensi pendidikan masif dan kolaborasi antarlembaga untuk mitigasi risiko jangka panjang.

Phishing toolkit merujuk pada paket perangkat lunak siap pakai yang memfasilitasi pembuatan situs web tiruan untuk mencuri informasi pribadi secara sistematis dan efisien. Secara teknis, toolkit ini mencakup script HTML, PHP, JavaScript, dan database yang meniru antarmuka autentik layanan seperti PayPal dengan fungsi capture data otomatis.[8] Dalam konteks hukum Indonesia, Pasal 34 UU ITE mendefinisikan produksi dan distribusi toolkit sebagai tindak pidana akses ilegal sistem elektronik dengan ancaman pidana maksimal 10 tahun penjara.[9] Terminologi pencucian uang (TPPU) melengkapi dengan Pasal 3 UU TPPU, di mana hasil penjualan toolkit dikonversi menjadi aset sah melalui cryptocurrency atau transfer bank anonim. Penggabungan kedua istilah ini mencerminkan

[2] Sameh Eltaybani, "Twenty Red Flags To Spot Phishing Emails from Predatory Journals," *Journal of Academic Ethics* 24, no. 1 (March 2026): 9, https://doi.org/10.1007/s10805-025-09679-z.
[3] Amanda Faizah; Jelita Putri Nurfahda Annasyanda; Yardi, Nayottama Aryasuta; Deni, Fitra, "ANALISIS PENIPUAN ONLINE DALAM BENTUK PHISING MENURUT PERSPEKTIF HUKUM INDONESIA," *SAHID BANKING JOURNAL*, no. Vol 4 No 1 (2024): OKTOBER 2024 (2024): 50–57, https://doi.org/10.56406/sahidbankingjournal.v4i1.193.
[4] Dewi Asri Puanandini, "PIDANA PENCUCIAN UANG HASIL KEJAHATAN SIBER (CYBER CRIME) MELALUI MATA UANG DIGITAL (CRYPTO CURRENCY)," *JURNAL PEMULIAAN HUKUM* 4, no. 2 (October 2021): 57–70, https://doi.org/10.30999/jph.v4i2.1480.
[5] Shaikha Ali Al Naqbi, Haitham Nobanee, and Nejla Ould Daoud Ellili, "Global Trends and Insights into Cryptocurrency-Related Financial Crime," *Research in International Business and Finance* 75 (March 2025): 102756, https://doi.org/10.1016/j.ribaf.2025.102756.
[6] Yazid Haikal Lokapala, Fuad Januar Nurfauzi, and Yeni Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 19–24, https://doi.org/10.18196/ijclc.v5i1.19853.
[7] Rahman, "ANALISIS DAN PENCEGAHAN SERANGAN SOSIAL ENGINERING PADA JARINGAN KOMPUTER STUDI KASUS PENIPUAN INVESTASI CRYPTO."
[8] Yukun Li et al., "A Stacking Model Using URL and HTML Features for Phishing Webpage Detection," *Future Generation Computer Systems* 94 (May 2019): 27–39, https://doi.org/10.1016/j.future.2018.11.004.
[9] Mohammad Yusuf and Maysarah, "Penerapan Hukum Terhadap Pelaku Kejahatan Tindak Pidana Akses Illegal," *Jurnal Pendidikan Dan Konseling* 4 (2022): 9735–40, https://doi.org/https://doi.org/10.31004/jpdk.v4i6.9920.

evolusi kejahatan siber hybrid yang memanfaatkan celah regulasi digital.[10] Definisi ini menjadi dasar pembuktian forensik dalam putusan pengadilan terkait barang bukti script dan mutasi rekening. Dengan demikian, pemahaman terminologi esensial untuk analisis kasus terpadu dan penegakan hukum efektif.

Kasus distribusi phishing toolkit menimbulkan masalah yuridis terkait kualifikasi Pasal 51 jo Pasal 35 UU ITE dan Pasal 3 UU TPPU dalam dakwaan kombinasi. Dakwaan ini memerlukan pembuktian ganda yaitu produksi toolkit sebagai fasilitasi kejahatan dan penyamaran asal harta kekayaan melalui aset seperti motor dan rekening tersangka.[11] Tuntutan Penuntut Umum sering kali kurang mempertimbangkan pembuktian terbalik aset, menyulitkan hakim dalam pertimbangan proporsionalitas hukuman dan pengembalian barang bukti.[12] Yuridisnya, bukti digital forensik seperti mutasi rekening BCA, script PHP, dan database 16shop krusial namun rentan kontestasi mengenai keotentikan dan rantai bukti.[13] Permasalahan ini diperparah oleh kurangnya harmonisasi regulasi cryptocurrency dengan TPPU, meskipun Indodax teridentifikasi sebagai saluran.[14] Pengembalian barang bukti seperti Honda Scoopy juga menimbulkan dilema keadilan restoratif versus rampasan negara. Masalah yuridis ini menekankan perlunya interpretasi progresif oleh putusan PN Banjarbaru untuk preseden ke depan.

## METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan mengombinasikan pendekatan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Pendekatan perundang-undangan digunakan untuk menelaah regulasi terkait kejahatan siber dan pencucian uang, khususnya ketentuan dalam Pasal 34, Pasal 35, jo Pasal 51 UU ITE serta Pasal 3 UU TPPU. Sementara itu, pendekatan kasus diterapkan melalui analisis mendalam terhadap Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb untuk membedah fakta hukum, pertimbangan majelis hakim, serta penerapan sanksi pidana terhadap terdakwa pelaku distribusi phishing toolkit. Kedua pendekatan ini didukung oleh sumber data sekunder—terdiri atas bahan hukum primer (regulasi dan putusan hakim), sekunder (literatur kejahatan siber, TPPU, dan teori kriminologi), serta tersier (kamus hukum dan glosarium siber)—yang dikumpulkan melalui teknik studi kepustakaan dan dianalisis secara kualitatif-deduktif dengan mengonfrontasikan norma hukum sebagai premis mayor terhadap fakta putusan sebagai premis minor guna mengevaluasi respon sistem peradilan pidana sekaligus merumuskan model pencegahan kriminologis yang tepat terhadap fenomena tersebut.

Penelitian mengenai phishing dan kejahatan siber telah berkembang dari kajian mengenai modus operandi menuju pembahasan mengenai komersialisasi perangkat kejahatan (crime toolkit) dan ekosistem Cybercrime-as-a-Service (CaaS). Alazab et al. menjelaskan bahwa perkembangan crime toolkit telah mengubah kejahatan siber menjadi komoditas yang dapat diperjualbelikan sehingga

[10] Nadia Wulandari Rotty et al., "Pemanfaatan Cryptocurrency Dalam Tindak Pidana Pencucian Uang," *Jurnal Hukum Statuta* 1, no. 2 (April 2022): 137–52, https://doi.org/10.35586/jhs.v1i2.8588.
[11] Tresia Elda, "TINJAUAN PROSES BEBAN PEMBUKTIAN TINDAK PIDANA MONEY LAUNDERING DI INDONESIA," *ADIL: Jurnal Hukum* 15, no. 1 (July 2024): 127–49, https://doi.org/10.33476/ajl.v15i1.4558.
[12] Patricia Edina Sembiring, "Menilai Pemberlakuan Pembuktian Terbalik Pada Tindak Pidana Pencucian Uang Sebagai Kejahatan Proxy Di Dalam Aset Kripto," *Integritas : Jurnal Antikorupsi*, June 2024, https://doi.org/10.32697/integritas.v10i1.1033.
[13] Sahuri Lasmadi and Elly Sudarti, "PEMBUKTIAN TERBALIK PADA TINDAK PIDANA PENCUCIAN UANG," *Refleksi Hukum: Jurnal Ilmu Hukum* 5, no. 2 (April 2021): 199–218, https://doi.org/10.24246/jrh.2021.v5.i2.p199-218.
[14] O S Wicaksono and S Mahmudah, "Analisis Hukum Cryptocurrency Sebagai Alat Pembayaran Di Indonesia: Perspektif Yuridis," *Jurnal Preferensi Hukum* 4, no. 2 (2023): 202–19, https://doi.org/https://doi.org/10.55637/jph.4.2.7147.202-219.

pelaku yang memiliki kemampuan teknis rendah tetap mampu melakukan serangan siber secara masif, namun penelitian tersebut lebih berfokus pada karakteristik teknis toolkit tanpa mengkaji pertanggungjawaban pidana maupun penegakan hukum terhadap pengembangnya.[15] Lee, Hur, dan Kim menganalisis struktur skrip pada phishing kit serta pengaruhnya terhadap penyebaran situs phishing di dunia nyata, tetapi penelitian tersebut menitikberatkan pada analisis keamanan siber dan deteksi teknis tanpa membahas dimensi kriminologis maupun pencucian uang yang timbul dari perdagangan toolkit tersebut.[16] Sementara itu, Kool, Moneva, dan Leukfeldt menunjukkan bahwa pasar Cybercrime-as-a-Service membentuk mekanisme kepercayaan yang mempermudah distribusi perangkat kejahatan kepada pelaku baru, namun kajian tersebut belum menghubungkannya dengan praktik penegakan hukum melalui putusan pengadilan.[17] Berdasarkan ketiga penelitian tersebut, kebaruan artikel ini terletak pada analisis terpadu mengenai komersialisasi phishing toolkit sebagai bentuk Cybercrime-as-a-Service yang dikaji melalui perspektif kriminologi dan hukum pidana dengan menggunakan Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb, sehingga mampu menjelaskan hubungan antara produksi perangkat kejahatan, eksploitasi finansial lintas negara, serta tindak pidana pencucian uang dalam satu konstruksi analisis.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis karakteristik komersialisasi *phishing toolkit* sebagai bentuk *Cybercrime-as-a-Service* serta mengkaji respons sistem peradilan pidana terhadap distribusi perangkat kejahatan siber dan tindak pidana pencucian uang yang menyertainya dalam Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN Bjb. Penelitian ini juga bertujuan menjelaskan keterkaitan antara kemampuan teknologi informasi yang dimiliki pelaku, motif ekonomi, dan pemanfaatan aset kripto sebagai sarana penyamaran hasil kejahatan dalam perspektif kriminologi modern. Kontribusi artikel ini bagi komunitas hukum pidana terletak pada pengembangan kajian mengenai pertanggungjawaban pidana terhadap pelaku yang mengomersialisasikan perangkat kejahatan siber, yang selama ini lebih banyak dibahas dari aspek teknis keamanan informasi dibandingkan aspek kebijakan hukum pidana. Temuan penelitian ini diharapkan dapat memperkaya pengembangan kebijakan penanggulangan kejahatan siber, khususnya dalam merumuskan strategi penegakan hukum terhadap ekosistem *Cybercrime-as-a-Service*, penguatan mekanisme perampasan aset hasil kejahatan siber, serta peningkatan efektivitas pemberantasan tindak pidana pencucian uang yang berasal dari kejahatan digital.

## DESKRIPSI KASUS

Kasus ini melibatkan Terdakwa bernama Riswanda Noor Saputra, seorang individu yang memiliki keahlian khusus di bidang informatika dan pemrograman komputer. Sejak sekitar tahun 2017 hingga 2019, Terdakwa secara aktif dan terencana merancang, mengembangkan, serta menguji sebuah perangkat lunak ilegal yang dikenal sebagai *phishing toolkit*. Dalam proses produksinya, Terdakwa memanfaatkan berbagai bahasa pemrograman seperti HTML, PHP, JavaScript, dan CSS untuk menciptakan produk piranti lunak komprehensif yang diberi nama "16Shop". Secara teknis, *phishing toolkit* 16Shop dirancang dengan tingkat kemiripan visual yang hampir sempurna untuk mereplikasi antarmuka autentik dari platform digital global terpercaya, seperti PayPal, Amazon, Apple, dan

[15] Ammar Alazab et al., "Crime Toolkits: The Productisation of Cybercrime," in *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*, 2013, 1626–32, https://doi.org/10.1109/TrustCom.2013.273.
[16] Rui Zhao et al., "Design and Evaluation of the Highly Insidious Extreme Phishing Attacks," *Computers & Security* 70 (September 2017): 634–47, https://doi.org/10.1016/j.cose.2017.08.008.
[17] Hannah Maartje Kool, Asier Moneva, and Rutger Leukfeldt, "Exploring Trust Signals and Pathways on Cybercrime-as-a-Service Markets: The Case of Remote Access Trojans," *Trends in Organized Crime*, July 2026, https://doi.org/10.1007/s12117-026-09606-7.

American Express. Piranti lunak ini dilengkapi dengan fitur *database* dan fungsi *capture data* otomatis. Melalui *script* yang dikembangkan oleh Terdakwa, para pembeli *toolkit* ini dapat mengirimkan email manipulatif dalam jumlah besar secara masif kepada calon korban untuk mengarahkan mereka ke situs web palsu (*pharming*) demi mencuri data kredensial pribadi secara efisien.[18] Meskipun pada perkembangannya Terdakwa menyadari bahwa piranti lunak tersebut digunakan untuk mengambil data pribadi dan informasi kartu kredit orang lain secara melawan hukum, ia tetap melanjutkan pengembangan dan penjualannya demi motif ekonomi. Terdakwa memasarkan produk tersebut secara komersial melalui sebuah situs web khusus. Untuk memfasilitasi transaksi ilegal ini, Terdakwa menyediakan metode pembayaran yang canggih berupa transfer bank anonim ke rekening BCA serta konversi mata uang digital melalui aset *bitcoin* di akun Indodax.

Aktivitas perdagangan *phishing toolkit* berskala internasional ini berhasil mendatangkan keuntungan finansial yang sangat besar bagi Terdakwa, dengan total akumulasi mencapai Rp1,7 miliar. Uang hasil kejahatan siber tersebut kemudian dikelola, dinikmati, dan disamarkan oleh Terdakwa ke dalam bentuk aset sah. Sebagian dari dana tersebut dikonversi menjadi barang-barang elektronik bernilai tinggi serta kendaraan bermotor, seperti laptop Lenovo Legion, Microsoft Surface Book, iPhone 11 Pro, dan sepeda motor Honda Scoopy. Tindakan penyamaran asal-usul harta kekayaan inilah yang memenuhi unsur materiil tindak pidana pencucian uang aktif. Dampak destruktif yang ditimbulkan oleh sindikat kejahatan siber ini bersifat multidimensional dan melintasi yurisdiksi nasional (*cybercrime* lintas negara). Distribusi massal *toolkit* 16Shop telah mengakibatkan kebocoran data sensitif dan kerugian finansial yang masif bagi ratusan ribu korban global, termasuk warga negara asing. Salah satu korban domestik yang teridentifikasi adalah Saksi Mari Ramadhan yang mengalami akses ilegal pada akun PayPal miliknya. Selain merugikan individu secara finansial dan psikologis, kasus ini juga mencatut merek dagang perusahaan multinasional serta mengikis kepercayaan publik terhadap ekosistem ekonomi digital. Skala kejahatan internasional yang masif ini akhirnya memicu perhatian global hingga melibatkan intervensi dari Interpol dan Kedutaan Besar Amerika Serikat dalam proses pengungkapannya. Kasus ini bermuara pada persidangan di Pengadilan Negeri Banjarbaru dengan nomor perkara 85/Pid.Sus/2022/PN Bjb. Dalam amar putusannya, Majelis Hakim menyatakan Terdakwa terbukti secara sah dan meyakinkan melanggar dakwaan kombinasi, yaitu Pasal 50 jo Pasal 34 ayat (1) huruf a UU ITE serta Pasal 3 UU TPPU. Atas perbuatannya, Terdakwa dijatuhi sanksi pidana pokok berupa penjara selama 2 tahun 6 bulan dan denda Rp500 juta, serta pidana tambahan berupa perampasan seluruh perangkat elektronik yang digunakan sebagai alat kerja kejahatan untuk dirampas bagi negara.

## PEMBAHASAN

### 1. Respon sistem peradilan pidana terhadap distribusi phishing toolkit dan tindak pidana pencucian uang yang menyertainya

Dalam perkara ini, Terdakwa Riswanda Noor Saputra terbukti membuat dan mengembangkan perangkat lunak berupa *phishing toolkit* sejak sekitar tahun 2017 hingga 2019, yang kemudian disempurnakan dan diperjualbelikan melalui situs tertentu untuk memperoleh keuntungan. Pada awalnya Terdakwa tidak mengetahui tujuan penggunaan software tersebut, namun dalam perkembangannya ia menyadari bahwa alat tersebut digunakan untuk memperoleh data pribadi orang

[18] Faiz Emery Muhammad and Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *Jurnal Usm Law Review* 6, no. 1 (2023): 226–41, https://doi.org/10.26623/julr.v6i1.6649.

lain secara ilegal, seperti data kartu kredit dan identitas pengguna. Meskipun demikian, Terdakwa tetap melanjutkan pengembangan dan penjualan software tersebut. Selain itu, Terdakwa juga menikmati dan mengelola hasil kejahatan tersebut, sehingga perbuatannya berkaitan pula dengan tindak pidana pencucian uang. Penuntut Umum menuntut agar Terdakwa dinyatakan bersalah melakukan tindak pidana di bidang Informasi dan Transaksi Elektronik serta tindak pidana pencucian uang, dan dijatuhi pidana penjara serta denda, dengan ketentuan subsider apabila denda tidak dibayar.

Dalam pertimbangannya, Majelis Hakim menilai bahwa unsur "dengan sengaja" telah terpenuhi karena Terdakwa mengetahui fungsi software yang dibuatnya dan tetap mengembangkan serta menjualnya. Unsur "tanpa hak atau melawan hukum" juga terpenuhi karena Terdakwa tidak memiliki kewenangan untuk mengakses dan memfasilitasi pengambilan data pribadi orang lain. Selain itu, unsur memproduksi atau menyediakan perangkat untuk melakukan kejahatan siber terbukti melalui pembuatan dan penjualan phishing toolkit tersebut. Hakim juga menilai bahwa unsur tindak pidana pencucian uang terpenuhi karena Terdakwa menikmati serta menyamarkan hasil kejahatan. Dalam menjatuhkan pidana, Hakim mempertimbangkan keadaan yang memberatkan, yaitu Terdakwa menikmati hasil kejahatan, menggunakan keahliannya untuk merugikan orang lain, serta perbuatannya menimbulkan keresahan bahkan hingga lintas negara. Adapun keadaan yang meringankan adalah Terdakwa belum pernah dihukum, mengakui perbuatannya, serta menunjukkan penyesalan. Berdasarkan seluruh pertimbangan tersebut, Majelis Hakim dalam amar putusannya menyatakan Terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana di bidang ITE dan pencucian uang, serta menjatuhkan pidana penjara dan denda, disertai penetapan terhadap barang bukti dan pembebanan biaya perkara kepada Terdakwa.

Perbuatan dilarang dalam putusan ini ada dua yaitu, mendistribusikan *toolkit phishing* dan pencucian uang pertama saya akan membahas distribusi *toolkit phishing* terlebih dahulu. Pada era moderm ini internet sangat mudah untuk diakases, kemudahan akses internet inilah yang dimanfaatkan oleh pelaku kejahatan siber yaitu *phishing.*[19] *Phishing* adalah salah satu jenis penipuan yang diperluas dimana pelaku meniru suatu identitas digunakan untuk memperoleh informasi dari target.[20] Di Indonesia memiliki beberapa peraturan yang mengatur kejahatan *phishing,* terutama Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pasal yang digunakan untuk menjerat pelaku dalam kejahatan ini antara lain pasal 28 ayat (1) dan pasal 35.[21] Dalam putusan ini untuk kejahatan *phishing* terdapat dua dakwaan yaitu, Pasal 50 ayat jo pasal 34 ayat (1) huruf a UU ITE 11/2008 dan 51 jo pasal 35 UU ITE 11/2008. Pasal yang paling cocok untuk kasus ini adalah pasal 50 ayat jo pasal 34 ayat (1) huruf a UU ITE 11/2008, karena dalam pasal tersebut berbunyi Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan, namun penuntut umum malah menggunakan pasal yang satunya dengan alasan terdakwa hanya menyediakan *script* yang dikembangkan khusus untuk melakukan phishing tersebut. Jadi distribusi *phishing toolkit*

[19] Mushlihudin Mushlihudin and Agil Nofiyan, "Analisis Forensik Pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," *Cybernetics* 4, no. 02 (2021): 11–23, https://doi.org/10.29406/cbn.v4i02.2287.
[20] Elmer E.H. Lastdrager, "Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature," *Crime Science* 3, no. 1 (2014): 1–10, https://doi.org/10.1186/s40163-014-0009-y.
[21] Putri Ramadhani Rangkuti et al., "Sanksi Pidana Terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia," *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi* 2, no. 3 (2025): 291–305, https://doi.org/10.62383/konstitusi.v2i3.908.

ini termasuk salah satu perbuatan yang dilarang karena tidak hanya menimbulkan kerugian finansial, tetapi juga dapat merusak reputasi dan kepercayaan publik.

Lalu perbutan selanjutnya ialah pencucian uang, tidak hanya di Indonesia hal ini juga menjadi perbuatan yang dilarang diberbagai negara. Pencucian uang merupakan kejahatan keuangan yang canggih hingga dapat menimbulkan ancaman signifikan terhadap integritas ekonomi dan keamanan nasional melalui penyamaran hasil kejahatan sebagai aset sah.[22] Kompleksitas skema pencucian uang di era modern menuntut kerangka yang menyeluruh yang dapat beradaptasi dengan tipologi baru dan inovasi teknologi. Di Indonesia sendiri sudah ada regulasi yang mengatur terkait tindak pidana ini yaitu Undang-Undang Nomor 15 Tahun 2002 yang telah diubah dengan Undang-Undang Nomor 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang, dan terakhir diubah dengan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-Undang ini sudah megatur dari bentuk, sistem pembuktian, hingga kewenangan PPATK.[23] Selain Undang-Undang di Indonesia juga ada sebuah lembaga seperti PPATK yang menjadi kunci dalam mendeteksi dan melaporkan sebuah transaksi yang mencurigakan.[24] Dalam putusan ini jaksa menggunakan bentuk pencucian uang aktif yang diatur dalam Pasal 3 UU No. 8 Tahun 2010, karena terdakwa melakukan transaksi dengan cara mentransfer kerekening BCA atau menggunakan *bitcoin* keakun indodax terdakwa. Tindak pidana pencucian uang ini dilarang karena berdampak merusak kestabilan ekonomi dan kerusakan reputasi negara.

Dalam hal hakim menjatuhkan putusan pemidanaan, salah satu hal yang harus termuat dalam putusan adalah hal yang memberatkan. Yang dimaksud dengan hal memberatkan menurut Hessick adalah segala fakta dan keadaan yang menjadi dasar diperberatnya pidana.[25] Hal memberatkan memiliki berbagai jenis yang sudah diatur dalam undang-undang, sehingga dalam menentukan pemberat harus dengan alasan objektif tidak bisa asal memilih.[26] Dalam putusan ini terdapat tiga hal yang memberatkan yang pertama terdakwa sudah menikmati hasil kejahatan, menggunakan keahliannya untuk merugikan orang lain, dan meresahkan masyarakat. Adanya pemberat pertama dan kedua ini karena *Phishing* memang dilakukan dengan cara yang membutuhkan keahlian dan bertujuan untuk mendapatkan keuntungan materiil maupun immateriil.[27] Untuk pemberat ketiga dikarenakan pada putusan ini terdakwa membuat web penjualan *software phishing* dan tidak sedikit pembelinya yang melakukan *phishing* tersebut sehingga meresahkan masyarakat. Dengan adanya tiga hal yang memberatkan tersebut terdakwa berpotensi terkena ancaman pidana yang tinggi, namun hal ini dapat di imbangi dengan hal yang meringankan.

Selain hal yang memberatkan ada juga yang disebut sebagai hal yang meringankan, hal ini memungkinkan hakim untuk menentukan berat ringannya pidana. Tetapi dalam hal tersebut harus didasarkan pada faktor-faktor yang meringankan.[28] Faktor-faktor yang dimaksud ialah perilaku pelaku

[22] Sahil Deswal, "Critical Analysis of Laws Related to Money Laundering and Its Prevention," *RESEARCH REVIEW International Journdskripsial of Multidisciplinary* 10, no. 5 (2025): 335–42, https://doi.org/10.31305/rrijm.2025.v10.n5.037.
[23] Riyanda Elsera, "KEBIJAKAN HUKUM PIDANA DALAM PEMBERANTASAN TINDAK PIDANA PENCUCIAN UANG DI INDONESIA," *Journal Equitable* 5 (2020), https://doi.org/https://doi.org/10.37859/jeq.v5i1.2464.
[24] Khadizah Aliyah Shiva, Salsabila Afifany Susanta Putry, and Asmak UI Hosnah, "Kebijakan Penegakan Hukum Tindak Pidana Terhadap Pencucian Uang (Money Laundering) Di Indonesia," *TATOHI: Jurnal Ilmu Hukum* 4, no. 10 (2024): 803, https://doi.org/10.47268/tatohi.v4i10.2581.
[25] Hananta Dwi, "Aggravating And Mitigating Circumstances Consideration On Sentencing," *Jurnal Hukum Dan Peradilan* 7, no. 1 (2018): 87.
[26] Larisa V. Gorbunova, Ruslan V. Makarov, and Sergei A. Matveev, "Aggravating Circumstances. Significance and Correlation with Qualifying Signs," *Mediterranean Journal of Social Sciences* 6, no. 3 (2015): 169–78, https://doi.org/10.5901/mjss.2015.v6n3s7p169.
[27] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."
[28] Fauzia Rahawarin et al., "Analisis Yuridis Pengurangan Hukuman Oleh Hakim Mahkamah Agung Dalam Perkara Tindak Pidana Korupsi Di Indonesia," *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 1 (2024): 423–35, https://doi.org/10.55606/jhpis.v3i1.4867.

kejahatan di masa lalu atau karakter yang baik dan saat ini atau penyesalan.[29] Dalam putusan ini terdakwa dinyatakan belum pernah dihukum serta mengaku bersalah dan menyesal lalu berjanji tidak akan mengulangi perbuatannya lagi. Untuk mengetahui apakah terdakwa benar – benar menyesal dan belum pernah dihukum, dapat diuji melalui salah satu tujuan pemidanaan yaitu rehabilitasi.[30] Yang dimaksud dengan rehabilitasi yaitu membuat pelaku kejahatan dapat memperbaiki diri dan dapat diterima kembali oleh lingkungan masyarakat dan mendapatkan hidup normal kembali. Berkat hal meringankan tersebut, dalam putusan hakim menghukum terdakwa dengan penjara 2 tahun 6 bulan dan denda 500 juta subsider 3 bulan.

Majelis hakim menjatuhkan pidana pokok penjara 2 tahun 6 bulan dan denda Rp. 500 Juta yang relevan dengan perbuatan terdakwa yaitu membuat dan menjual phishing toolkit. Penjatuhan Pidana ini sesuai dengan Pasal 50 jo Pasal 34 ayat (1) huruf a UU Informasi Transaksi Elektronik dan Pasal 3 Undang-Undang Tindak Pidana Pencucian Uang yang terbukti dari bukti digital dan keterangan saksi. Pidana penjara dalam kasus ini dilakukan untuk menimbulkan efek jera kepada pelaku seperti dalam kasus kejahatan siber yang merugikan banyak korban seperti pencurian data PayPal dan kartu kredit.[31] Majelis hakim juga menetapkan nominal denda yang sebanding dengan keuntungan finansial yang diperoleh oleh terdakwa dari transaksi ilegal.[32] Ketentuan Subsidair kurungan selama 3 bulan diberikan untuk memaksa terdakwa membayar penuh denda yang diberikan atau menjalani tambahan hukuman sesuai dengan Pasal 30 KUHP. Pemilihan pidana pokok ini adil karena seimbang antara pidana dan faktor pribadi terdakwa di persidangan yang membenarkan sebagian bukti. Dalam kasus ini dakwaan kumulatif ITE dan TPPU terbukti penuh tanpa cacat formil karena kesesuaian bukti dengan dakwaan yang memenuhi asas *ne bis in idem*.

Pidana pokok ini relevan karena melindungi keamanan siber nasional dari ancaman phishing toolkit, serta mempertimbangkan dampak luas termasuk laporan FBI dan kerugian korban asing. Dalam kasus ini penjatuhan pidana kepada terdakwa lebih berat dari tuntutan Jaksa Penuntut Umum yaitu 1 tahun penjara dan denda Rp200 juta yang menunjukkan adanya pertimbangan yang matang atas barang-barang bukti yang ada.[33] Hal ini sejalan dengan praktik Majelis Hakim dalam kasus Informasi Transaksi Elektronik yang tegas untuk efek deterensi.[34] Sanksi pidana ini mencakup aspek Tindak Pidana Pencucian Uang dari aliran dana hasil dari penjualan software.[35] Pengadilan memastikan proporsionalitas dengan merujuk pada analisis Pusat Pelaporan Analisis Transaksi Keuangan atas pola transaksi yang mencurigakan. Pidana denda menargetkan pemulihan kerugian korban seperti Saksi Mari Ramadhan atas akses ilegal PayPal-nya. Secara keseluruhan, pidana pokok tersebut memperkuat keadilan restoratif dalam kasus siber lintas yurisdiksi.

Majelis hakim dalam kasus ini menyatakan pidana perampasan barang terhadap 1 unit laptop Microsoft Surface Book, 1 unit laptop Lenovo Legion Y545 beserta harddisk 1 TB, 1 unit handphone iPhone 11 Pro, serta 2 buah SIM card dan 2 buah flashdisk sebagai pidana tambahan yang relevan.

[29] Ian K. Belton and Mandeep K. Dhami, "The Role of Character-Based Personal Mitigation in Sentencing Judgments," *Journal of Empirical Legal Studies* 21, no. 1 (2024): 208–39, https://doi.org/10.1111/jels.12376.
[30] Ahmad Iqbal, "Merasionalkan Keadaan Yang Meringankan Pada Putusan Hakim Di Indonesia," *Jurnal Media Hukum* 13, no. 2 (2025): 303–13, https://doi.org/10.59414/jmh.v13i2.1048.
[31] Antara Norma et al., "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Phising Di Indonesia (Studi Kasus Putusan Pengadilan Negeri Banjarbaru No 85/Pid.Sus/2022/PN Bjb)," *Jurnal Hukum Pidana, Kriminologi Dan Viktimologi* 1, no. 2 (2024): 62–78.
[32] Muhammad and Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web."
[33] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."
[34] Afifah Sahfitri and Rosmalinda Rosmalinda, "Penipuan Digital Melalui Tautan Phishing," *Jurnal Dialektika Hukum* 6, no. 2 (2024): 92–107, https://doi.org/10.36859/jdh.v6i2.2881.
[35] Gift Onwuadiamu, "Cybercrime in Criminology; A Systematic Review of Criminological Theories, Methods, and Concepts," *Journal of Economic Criminology* 8, no. December 2024 (2025): 100136, https://doi.org/10.1016/j.jeconc.2025.100136.

Barang-barang tersebut dirampas untuk negara karena telah digunakan langsung dalam produksi dan penjualan software phishing toolkit 16Shop, yang menghasilkan keuntungan ekonomi mencapai Rp1,7 miliar bagi terdakwa. Majelis hakim menilai barang-barang itu memiliki nilai ekonomi tinggi dan merupakan hasil tindak pidana pencucian uang serta manipulasi data elektronik.[36] Pidana perampasan ini proporsional mengingat motif ekonomi terdakwa, di mana ia menjual software ilegal karena kesulitan finansial keluarga.[37] Penggunaan laptop dan flashdisk untuk mengembangkan kode PHP, HTML, serta menyimpan data korban menjadikan perampasan sebagai pencegahan pengulangan kejahatan.[38] iPhone dan SIM card juga relevan karena terhubung dengan akun email serta transaksi pembayaran seperti Indodax. Dengan demikian, keputusan majelis hakim selaras dengan Pasal 50 UU ITE dan Pasal 3 UU TPPU untuk menghilangkan sarana kejahatan.

Meskipun terdakwa mengaku bersalah dan menyesal akibat ketiadaan pekerjaan sesuai ilmu informatika, perampasan tetap relevan karena barang-barang tersebut dibeli dari hasil penjualan software ilegal. Majelis hakim menolak pengembalian barang meski terdakwa memohon keringanan dengan alasan kebutuhan hidup, karena aset seperti laptop bernilai jutaan rupiah telah dimanfaatkan untuk kejahatan siber skala internasional.[39] Nilai ekonomi barang yang dirampas, seperti iPhone senilai belasan juta, mencerminkan keuntungan motif ekonomi terdakwa yang mengakibatkan kerugian korban global.[40] Pidana ini efektif mencegah terdakwa mengulangi kejahatan, sebab perangkat tersebut esensial dalam pengujian dan distribusi toolkit phishing.[41] Namun, majelis hakim membedakan dengan mengembalikan KTP dan buku tabungan, menunjukkan pertimbangan proporsionalitas. Secara keseluruhan, perampasan memperkuat efek jera terhadap kejahatan cyber dengan motif ekonomi seperti kasus ini. Keputusan ini juga konsisten dengan tuntutan penuntut umum untuk memusnahkan atau merampas barang bukti berpotensi berbahaya.

Secara yuridis, konstruksi perkara ini menunjukkan penerapan pidana kumulatif yang solid antara kejahatan siber (phishing) dan tindak pidana pencucian uang (TPPU). Putusan Majelis Hakim mempertegas bahwa pembuatan serta pendistribusian phishing toolkit seperti script 16Shop memenuhi unsur kesengajaan dan sifat melawan hukum (wederrechtelijk) dalam UU ITE, di mana terdakwa secara sadar memfasilitasi kejahatan komputer yang merugikan korban hingga skala internasional. Penjeratan Pasal 34 jo. Pasal 50 UU ITE terbukti paling tepat dibandingkan pasal deskriptif biasa karena secara spesifik melarang penyediaan perangkat lunak yang dirancang untuk kejahatan TIK. Terlebih lagi, integrasi Pasal 3 UU TPPU mengonfirmasi adanya pencucian uang aktif, di mana transaksi hasil kejahatan yang disalurkan melalui rekening bank dan dompet aset kripto (Indodax) dianalisis oleh PPATK sebagai bentuk penyamaran asal-usul kekayaan yang merusak stabilitas sistem keuangan.

Ratio decidendi Majelis Hakim dalam menjatuhkan sanksi yang lebih berat dari tuntutan Jaksa Penuntut Umum yakni 2 tahun 6 bulan penjara dan denda Rp500 juta merupakan wujud nyata penegakan efek deterensi (deterrence effect) terhadap cybercrime bermotif ekonomi tinggi. Dalam

[36] Lasmadi and Sudarti, "PEMBUKTIAN TERBALIK PADA TINDAK PIDANA PENCUCIAN UANG."
[37] Dina Putri, "Penerapan Perampasan Aset Sebagai Tambahan Dalam Tindak Pidana Korupsi Indonesia," *Jurnal Hukum Samudra Keadilan* 19, no. 2 (2024): 302–19.
[38] Arizon Mega Jaya, "Implementasi Perampasan Harta Kekayaan Pelaku Tindak Pidana Korupsi (Implementation of Asset Deprivation of Criminal Act of Corruption)," *Cepalo* 1, no. 1 (2017): 19–28, https://doi.org/10.25041/cepalo.v1no1.1752.
[39] Gumilang Fuadi, Windy Virdinia Putri, and Trisno Raharjo, "Tinjauan Perampasan Aset Dalam Tindak Pidana Pencucian Uang Dari Perspektif Keadilan," *Jurnal Penegakan Hukum Dan Keadilan* 5, no. 1 (March 2024): 53–68, https://doi.org/10.18196/jphk.v5i1.19163.
[40] Lonna Yohanes Lengkong, "Urgensi Penerapan Perampasan Aset Dalam Tindak Pidana Pencucian Uang," *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 3 (December 2023): 351–64, https://doi.org/10.55809/tora.v9i3.278.
[41] PSHK, "Penjelasan Hukum Tentang Perampasan Aset Tanpa Pemidanaan," *PSHK Restatement*, 2019.S

menimbang sanksi, hakim secara proporsional mengonfrontasikan faktor memberatkan (dampak keresahan global dan pemanfaatan keahlian khusus) dengan faktor meringankan (pengakuan, penyesalan, dan status belum pernah dihukum) guna mendukung efektivitas rehabilitasi hukum. Keadilan substantif semakin diperkuat melalui pidana tambahan berupa perampasan barang bukti bernilai tinggi (laptop, smartphone, dan media penyimpanan) untuk negara. Tindakan perampasan aset (asset forfeiture) ini tidak hanya merampas alat yang digunakan (instrumenta sceleris), tetapi juga melumpuhkan sarana ekonomi utama pelaku guna mencegah keberlanjutan atau pengulangan kejahatan serupa di masa depan

### 2. Karakteristik komersialisasi phishing toolkit sebagai bentuk cybercrime-as-a-service dalam Putusan Nomor 85/Pid.Sus/2022/PN Bjb

Berdasarkan putusan pengadilan, terdakwa Riswanda Noor Saputra melakukan tindak pidana siber dengan cara membuat dan menjual phishing tool kit melalui website 16Shop yang secara aktif merancang, mengembangkan, dan menguji tool tersebut menggunakan kemampuan pemrograman seperti HTML, PHP, JavaScript, dan CSS hingga dapat berfungsi dengan baik. Kemudian tool tersebut dipasarkan kepada pihak lain untuk melakukan penipuan terhadap korban dan terdakwa juga menyediakan berbagai metode pembayaran dalam pemasaran tool tersebut yaitu transfer bank dan cryptocurrency, yang menunjukkan adanya orientasi untuk memperoleh keuntungan finansial. Perbuatan ini dilakukan secara sadar dan terencana, mengingat terdakwa mengetahui bahwa tool yang dijual akan digunakan untuk mencuri data pribadi dan informasi keuangan korban. Dengan demikian, motivasi pelaku dapat dipahami sebagai upaya memperoleh keuntungan ekonomi dengan memanfaatkan kemampuan teknis yang dimiliki secara melawan hukum.

Keadaan yang menyebabkan timbulnya korban dalam perkara ini berkaitan dengan penggunaan phishing tool kit yang dirancang menyerupai tampilan asli layanan digital aplikasi seperti PayPal, Apple, dan Amazon. Berdasarkan putusan, pembeli tool tersebut mengirimkan email dalam jumlah besar kepada calon korban dengan isi pemberitahuan akun terkunci atau aktivitas mencurigakan sehingga mengakibatkan kepanikan bagi korban. Korban yang menerima email tersebut kemudian diarahkan untuk mengklik tautan yang mengarah ke website palsu yang tampilannya sangat mirip dengan situs resmi. Hal tersebut membuat korban percaya sehingga korban dapat memasukkan data pribadi dan juga informasi kartu kredit mereka. Data tersebut kemudian disimpan dan dapat digunakan untuk kepentingan ilegal seperti transaksi atau penjualan data oleh pembeli tool. Dengan demikian, timbulnya korban dalam kasus ini disebabkan oleh kurangnya kewaspadaan korban dalam memverifikasi informasi yang diterima serta kesadaran terhadap kemajuan teknologi yang semakin pesat yang membuat korban menjadi mudah tertipu.

Faktor yang melatarbelakangi terjadinya kasus ini dapat dilihat dari putusan yang menjelaskan bahwa terdakwa membuat dan menjual phishing tool kit untuk mencuri data akun dan kartu kredit seseorang bagi yang membelinya. Menurut David J. Lemay menjelaskan bahwa phishing muncul sebagai salah satu bentuk kejahatan siber yang dilakukan dengan teknik penipuan yang menggunakan kombinasi rekayasa sosial dan teknologi untuk mengumpulkan informasi sensitif dan pribadi dengan menyamar sebagai orang atau bisnis yang dapat dipercaya dalam komunikasi elektronik seperti pesan SMS, email, dan komunikasi suara,[42] sehingga dengan berkembangnya teknologi digital dan

[42] David J. Lemay, Ram B. Basnet, and Tenzin Doleck, "Examining the Relationship between Threat and Coping Appraisal in Phishing Detection among College Students," *Journal of Internet Services and Information Security* 10, no. 1 (2020): 38–49, https://doi.org/10.22667/JISIS.2020.02.29.038.

meningkatnya penggunaan media social di dunia digital memberikan peluang bagi pelaku untuk menjalankan aksinya demi keuntungan secara ilegal.[43] Yazid Hikal Lokapala juga menjelaskan bahwa Phishing merupakan tindakan penipuan yang dilakukan secara daring bertujuan memperoleh informasi pribadi dan modus yang dilakukan dengan memanfaatkan teknik sosial, manipulasi, dan teknologisehingga dapat merugikan individu dan organisasi.[44] Menurut Fitaria Bantara, dkk, pelaku phishing biasanya mempelajari keterampilan teknis melalui interaksi dengan kelompok kejahatan siber sehingga kejahatan ini tidak dilakukan secara spontan, melainkan melalui proses pembelajaran yang memungkinkan pelaku memanfaatkan teknologi canggih dan jaringan internet untuk membuat serta menyebarkan alat phishing demi memperoleh keuntungan ekonomi.[45] Dalam penelitian Sitti Aiman menjelaskan bahwa kejahatan phishing dilakukan karena pelaku memanfaatkan kemudahan dalam menipu individu yang cenderung mempercayai sumber yang tampak resmi serta kelemahan psikologis berupa kepanikan dan pengambilan keputusan yang tidak rasional, sehingga memungkinkan pelaku memperoleh keuntungan secara cepat.[46] Maka dapat disimpulkan bahwa kasus ini terjadi karena pelaku memanfaatkan perkembangan teknologi digital dan kemampuan teknis di bidang komputer untuk membuat dan menjual phishing tool kit yang digunakan mencuri data korban demi memperoleh keuntungan ekonomi secara ilegal.

Faktor lain yang mempengaruhi pelaku melakukan kejahatan siber seperti phishing juga dapat dilihat dari ideologi yang tercipta pada diri pelaku, seperti tujuan yang ingin dicapai sehingga pelaku melakukan teknik kejahatan untuk mencapai tujuan yang diinginkan. Hal tersebut sesuai dengan pendapat Marco Romagna, dkk yang menjelaskan bahwa keterlibatan seseorang dalam aktivitas peretasan tidak hanya didorong oleh faktor teknis, tetapi juga oleh faktor sosial, psikologis, dan ideologis yang saling berkaitan,[47] salah satu contohnya yaitu pelaku merasa terdorong oleh keyakinan bahwa tindakan yang mereka lakukan dapat membawa perubahan sehingga kemampuan teknis yang mereka miliki digunakan sebagai alat untuk mencapai tujuan sekaligus memperkuat identitas diri.[48] Dalam kasus tersebut pelaku membuat dan memperjualbelikan alat (phishing tool kit) yang digunakan untuk membuat tampilan website palsu menyerupai layanan resmi guna mengelabui korban agar memberikan data pribadi. Maka jenis phishing yang dilakukan oleh pelaku disebut pharming, pharming adalah serangan kejahatan siber yang bertujuan untuk mengalihkan lalu lintas internet pengguna ke situs web palsu dengan cara memanipulasi sistem DNS *(Domain Name System)* atau mengubah pengaturan file hosts pada komputer pengguna.[49] Selain itu menurut Xuecong Lu phishing masih menjadi kejahatan siber yang banyak terjadi karena meskipun teknologi keamanan sudah berkembang masih ada pesan berbahaya yang lolos dan sulit dikenali pengguna terutama ketika mereka sedang melakukan banyak aktivitas secara bersamaan.[50] Maka dapat disimpulkan bahwa

[43] Nailah + S and Rosnelly + R, "Analisis Ancaman PhishingDi PlatformMedia Sosial Emailmenggunakan Metode Digital Forensic Research Workshop," *Rekayasa Sistem* 3, no. 2 (2025): 450–61.
[44] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."
[45] Fitaria Bantara et al., "Analisis Kriminologi Atas Kejahatan Dunia Maya Phising Di Era Pandemi Covid-19," *Birokrasi: JURNAL ILMU HUKUM DAN TATA NEGARA* 3, no. 1 (March 2025): 10–20, https://doi.org/10.55606/birokrasi.v3i1.1801.
[46] Freyha A Bahari et al., "The Psychology of Phishing: Why Users Fall Victim to Deceptive Emails," *International Journal of Innovative Science and Research Technology* 9, no. 12 (2024): 10–12.
[47] Marco Romagna and Rutger E. Leukfeldt, "Becoming a Hacktivist. Examining the Motivations and the Processes That Prompt an Individual to Engage in Hacktivism," *Journal of Crime and Justice* 47, no. 4 (August 2024): 511–29, https://doi.org/10.1080/0735648X.2023.2216189.
[48] Thomas J. Holt, Joshua D. Freilich, and Steven M. Chermak, "Exploring the Subculture of Ideologically Motivated Cyber-Attackers," *Journal of Contemporary Criminal Justice* 33, no. 3 (August 2017): 212–33, https://doi.org/10.1177/1043986217699100.
[49] Irwan Darmawan et al., "Analisis Pharming Dalam Cyber Crime Di Layanan Mobile Banking," *Jurnal Informasi Dan Teknologi* 5, no. 2 (2023): 159–63, https://doi.org/10.37034/jidt.v5i2.362.
[50] Xuecong Lu et al., "Phishing Detection in Multitasking Contexts: The Impact of Working Memory Load, Goal Activation, and Message Framing Cue on Detection Performance," *European Journal of Information Systems* 35, no. 1 (January 2026): 134–64, https://doi.org/10.1080/0960085X.2025.2548543.

pelaku memiliki tujuan tertentu yang ingin dicapai sehingga memanfaatkan kesempatan untuk melakukan kejahatan disaat korban sedang lengah dengan banyak aktivitas lain yang pada akhirnya pelaku berhasil mengelabuih korban.

Faktor yang melatarbelakangi timbulnya korban dalam kasus phishing adalah rendahnya tingkat literasi digital masyarakat dalam mengenali bentuk penipuan di ruang siber. Menurut Lutfi Aziz, dkk menjelaskan bahwa korban phishing dapat terjadi karena kesalahan manusia, kelengahan dalam menjaga keamanan informasi, keterbatasan pengelolaan sistem keamanan siber, serta kemampuan pelaku memanfaatkan perkembangan teknologi untuk mengeksploitasi kelemahan tersebut,[51] sehingga menurut penelitian yang dikemukakan oleh Ahmad Maulana Fikri bahwa diperlukannya edukasi bagi Masyarakat untuk meningkatkan kesadaran dan kemampuan masyarakat dalam mengenali terkait ancaman phishing dan tindakan untuk menghindarinya.[52] Selain kelemahan mereka tentang literasi digital mengenali bentuk ancaman phishing, kurangnya pemahaman mereka mengenai panduan penggunaan fitur keamanan bagi pengguna sosial media juga menjadi faktor yang dapat menjadikan mereka korban kejahatan siber.[53] Pentingnya keamanan siber perlu dipahami oleh seluruh pengguna komputer karena meningkatnya penggunaan internet dalam kehidupan sehari-hari juga diikuti dengan meningkatnya berbagai ancaman siber seperti malware, spam, serangan DDoS, rekayasa sosial, dan phishing yang memanfaatkan kelemahan sistem maupun kelalaian pengguna untuk memperoleh keuntungan tertentu.[54] Ketika suatu organisasi tidak memiliki kebijakan keamanan yang kuat, pengguna tidak memiliki perilaku keamanan yang baik, dan teknologi pendukung belum memadai, maka sistem menjadi lebih rentan sehingga peluang terjadinya serangan siber dan timbulnya korban menjadi lebih besar.[55] Maka dapat disimpulkan bahwa timbulnya korban dalam kasus phishing dipengaruhi oleh rendahnya literasi digital, kelalaian pengguna dalam menjaga keamanan informasi, serta lemahnya sistem dan kebijakan keamanan siber yang membuat pelaku lebih mudah mengeksploitasi kelemahan tersebut.

Faktor lain yang dapat melatarbelakangi timbulnya korban dalam kasus phishing adalah kondisi psikologis pengguna yang dapat mempengaruhi cara mereka merespons informasi atau pesan yang diterima di ruang digital. Penelitian yang dilakukan oleh Helen S. Jones menunjukkan bahwa faktor psikologis individu seperti impulsivitas, tingkat kepercayaan, dan cara memproses informasi dapat memengaruhi kerentanan seseorang terhadap penipuan email dan phishing,[56] sehingga orang yang lebih impulsif atau kurang teliti dalam mengevaluasi pesan yang diterima akan cenderung lebih mudah tertipu.[57] Viktimisasi phishing tidak selalu disebabkan oleh kurangnya pengetahuan karena meskipun korban memiliki pemahaman tentang penipuan mereka tetap dapat terpengaruh oleh faktor emosional dan rangsangan psikologis yang memengaruhi perilaku tanpa disadari.[58] Liliana Ribeiro mengemukakan bahwa individu yang merasa tidak yakin dengan kemampuannya atau

[51] Lutfi Aziz Febrika Ardy et al., "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial," *Journal of Internet and Software Engineering* 1, no. 4 (June 2024): 11, https://doi.org/10.47134/pjise.v1i4.2753.
[52] Fitaria Bantara et al., "Analisis Kriminologi Atas Kejahatan Dunia Maya Phising Di Era Pandemi Covid-19."
[53] Jason Matthew Sutanto and Nadia Nadia, "Cyber Security Awareness Simulation for Web Phishing in E-Commerce," *Engineering, MAthematics and Computer Science Journal (EMACS)* 7, no. 1 (January 2025): 69–78, https://doi.org/10.21512/emacsjournal.v7i1.12100.
[54] Nalin Asanka Gamagedara Arachchilage and Steve Love, "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective," *Computers in Human Behavior* 38 (September 2014): 304–12, https://doi.org/10.1016/j.chb.2014.05.046.
[55] Chrispus Zacharia Oroni and Fu Xianping, "Evaluating the Influence of Cybersecurity Policies and Cybersecurity Behavior on Institutional Security Performance in Remote Learning: The Moderating Role of Technological Readiness," *Sustainable Futures* 10 (December 2025): 101554, https://doi.org/10.1016/j.sftr.2025.101554.
[56] Helen S. Jones et al., "Email Fraud: The Search for Psychological Predictors of Susceptibility," *PLoS ONE* 14, no. 1 (2019): 1–15, https://doi.org/10.1371/journal.pone.0209684.
[57] Dawn M. Sarno, Maggie W. Harris, and Jeffrey Black, "Which Phish Is Captured in the Net? Understanding Phishing Susceptibility and Individual Differences," *Applied Cognitive Psychology* 37, no. 4 (July 2023): 789–803, https://doi.org/10.1002/acp.4075.
[58] Arachchilage and Love, "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective."

rendahnya kepercayaan pada dirinya dalam mendeteksi ancaman digital akan lebih rentan tertipu, maka dari itu kepercayaan diri seseorang dalam mendeteksi phishing juga berpengaruh besar terhadap kerentanan seseorang menjadi korban phishing.[59] Selain faktor psikologis yang mempengaruhi bagaimana masyarakat bertindak terhadap ancaman phishing yang mereka terima, kejahatan phising juga sangat berpengaruh terhadap dampak psikologis yang didapatkan korban yaitu merasakan khawatir, ketiknyamanan, cemas dan gangguan mental lain akibat kerugian yang didapatnya.[60] Maka dapat disimpulkan bahwa timbulnya korban dalam kasus phishing juga dapat dipengaruhi oleh kondisi psikologis individu yang dapat membuat seseorang lebih mudah tertipu oleh pesan atau informasi palsu sehingga menimbulkan korban baru lainnya.

Kasus phising tool kit 16Shop menimbulkan dampak destruktif yang signifikan terhadap korban, terutama dalam aspek kerugian finansial dan pelanggaran privasi data pribadi. Korban yang membuka halaman login palsu tanpa sadar telah memberikan data sensitif seperti kata sandi, nomor kartu kredit, serta identitas pribadi yang dapat disalahgunakan pelaku.[61] Informasi pribadi yang diperoleh melalui phising tool kit tersebut dapat dimanfaatkan untuk melakukan penipuan finansial lanjutan, termasuk transaksi ilegal yang secara langsung merugikan korban.[62] Selain menimbulkan kerugian materiil, serangan phising juga memanfaatkan manipulasi psikologis melalui email palsu yang membuat korban merasa terjadi aktivitas tidak wajar pada akun mereka, seolah-olah kesalahan berasal dari korban sendiri.[63] Besarnya skala serangan yang melibatkan ratusan ribu email menunjukkan bahwa ancaman terhadap perlindungan data pribadi masyarakat telah berada pada tingkat yang sangat mengkhawatirkan serta eksploitatif. Lebih lanjut, data yang telah bocor berpotensi terus beredar dan diperjualbelikan di berbagai situs pasar gelap bahkan setelah kasus terungkap. Dengan demikian, kasus 16Shop membuktikan bahwa phishing tool kit mampu menimbulkan dampak destruktif multidimensi yang mencakup kerugian finansial sekaligus pelanggaran privasi korban secara masif.

Selain berdampak pada korban individu, kasus phising ini juga menimbulkan implikasi serius terhadap kepercayaan publik pada ekosistem digital serta stabilitas layanan keuangan global. Perusahaan besar seperti Apple, Amazon, PayPal, dan American Express juga turut menjadi korban pencatutan merek karena sistem yang dibuat terdakwa mampu mereplikasi tampilan situs resmi mereka.[64] Akibatnya, praktik illegal ini secara kolektif berkontribusi mengikis kepercayaan publik global terhadap keamanan transaksi ekonomi digital serta integritas sistem informasi daring.[65] Lebih lanjut, penyebaran komersial phishing tool kit oleh terdakwa turut membentuk ekosistem kejahatan siber terorganisir, di mana pelaku lain dengan kemampuan teknis terbatas dapat melancarkan

[59] Liliana Ribeiro, Inês Sousa Guedes, and Carla Sofia Cardoso, "Which Factors Predict Susceptibility to Phishing? An Empirical Study," *Computers & Security* 136 (January 2024): 103558, https://doi.org/10.1016/j.cose.2023.103558.
[60] Indah Siti Saidah, "Keamanan Digital Dalam Perspektif Al-Qur'an: Kasus Kejahatan Phishing," *Mashadiruna Jurnal Ilmu Al-Qur'an Dan Tafsir* 3, no. 2 (October 2024): 109–14, https://doi.org/10.15575/mjiat.v3i2.34819.
[61] Sanjok Subedi. Swarnalatha, KC. Ramchandra, KC. Anshari, Kaushar. Ojha, Love. Sharma, "Real-Time Threat Intelligence-Block Phising Attacks," *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2021, https://doi.org/10.1109/CSITSS54238.2021.9683237.
[62] Naresh Kamble & Nilamadhab Mishra, "Hybrid Optimization Enabled Squeeze Net for Phishing Attack Detection," *Computers & Security* 144 (2024), https://doi.org/https://doi.org/10.1016/j.cose.2024.103901.
[63] Aulia Anjani Nurdin, Axara Alejendra Anjani, and Fiqih Dien Alamsyah, "Media Hukum Indonesia ( MHI ) Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi Media Hukum Indonesia ( MHI )" 2, no. 2 (2024): 74–82, https://doi.org/https://doi.org/10.5281/zenodo.11183088.
[64] Meenu Chawla & Namita Tiwari Richa Goenka, "A Comprehensive Survey of Phishing: Mediums, Intended Targets, Attack and Defence Techniques and a Novel Taxonomy," *International Journal of Information Security* 23 (2024): 819–48, https://doi.org/https://doi.org/10.1007/s10207-023-00768-x.
[65] Morice Daudi, "Exploiting Human Trust in Cybersecurity: Which Trust Development Process Is Predominant in Phishing Attacks?," *Applied Cybersecurity and Internet Governance* 3, no. 2 (2024): 233–49, https://doi.org/10.60097/ACIG/199452.

serangan phishing yang masif.[66] Hal ini tentunya memperluas jangkauan kejahatan siber melampaui yurisdiksi nasional, sehingga meningkatkan kompleksitas penanganan serta koordinasi lembaga penegak hukum lintas negara dalam penyelidikan dan penuntutan. Keterlibatan Interpol dan Kedutaan Besar Amerika Serikat dalam pengungkapan kasus ini membuktikan bahwa kejahatan siber asal Indonesia telah menimbulkan kerugian yang dirasakan secara internasional. Dengan demikian, kasus phishing tool kit 16Shop menegaskan terkait urgensi penguatan regulasi siber, kolaborasi antarnegara, serta peningkatan literasi digital sebagai respons komprehensif terhadap ancaman kejahatan siber terorganisir

## SIMPULAN

Penguatan literasi digital merupakan kunci utama dalam upaya memutus rantai keberhasilan serangan *phishing* yang mengeksploitasi kerentanan para pengguna berbagai platform digital. Program edukasi keamanan siber sebaiknya diintegrasikan ke dalam kurikulum pendidikan dan pelatihan kerja sehingga dapat membangun kesadaran kritis terhadap berbagai modus kejahatan digital era modern. Upaya edukasi ini harus difokuskan pada pengenalan ciri-ciri situs palsu serta pentingnya melakukan verifikasi dua langkah guna melindungi kredensial pribadi dari ancaman pencurian data. Selain itu, pemerintah bersama penyedia platform perlu mengadakan kampanye edukatif mengenai bahaya membagikan informasi sensitif melalui tautan tidak resmi yang dikirimkan melalui email mencurigakan. Sinergi antara sektor publik dan swasta juga diperlukan dalam penyebaran konten edukatif yang mudah dipahami sehingga membentuk masyarakat digital yang lebih waspada terhadap berbagai manipulasi informasi. Pencegahan kejahatan yang efektif harus berakar pada penanganan faktor sosial, ekonomi, dan budaya yang melatarbelakangi muncul serta berkembangnya perilaku kriminal di masyarakat. Oleh karena itu, pembangunan kapasitas intelektual masyarakat dalam menyaring informasi digital menjadi fondasi paling krusial untuk mencegah meluasnya praktik penipuan daring di masa akan datang.

Penguatan infrastruktur keamanan siber secara teknis juga menjadi langkah strategis dalam upaya pencegahan untuk membatasi dan menanggulangi penyebaran serangan *phishing* secara luas di lingkungan digital. Penyedia layanan digital dapat mengintegrasikan sistem deteksi otomatis berbasis kecerdasan buatan guna mengidentifikasi serta memblokir penggunaan *script* berbahaya yang memiliki ciri khas sebagai alat *phishing*. Selain itu, penguatan protokol otentikasi bagi pengelola domain menjadi langkah penting untuk menghambat pelaku kejahatan siber dalam meniru identitas visual perusahaan besar yang terpercaya. Standardisasi protokol keamanan siber nasional juga seharusnya mewajibkan seluruh platform digital menerapkan keamanan berlapis sehingga mempersempit celah teknis yang selama ini dieksploitasi pelaku kejahatan siber. Kolaborasi antara platform digital dan penyedia layanan hosting dalam membangun sistem pelaporan terpadu memungkinkan proses takedown situs phishing dilakukan secara lebih cepat dan terkoordinasi. Penerapan sistem pemantauan domain secara real-time oleh lembaga siber juga dapat mendeteksi keberadaan situs tiruan sebelum berhasil menjangkau dan merugikan pengguna yang menjadi targetnya. Dengan demikian, penguatan infrastruktur keamanan siber secara teknis dan sistematis

[66] Woonghee Lee, Junbeom Hur, and Doowon Kim, *Beneath the Phishing Scripts: A Script-Level Analysis of Phishing Kits and Their Impact on Real-World Phishing Websites*, *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, vol. 1 (Association for Computing Machinery, 2024), https://doi.org/10.1145/3634737.3657013.

merupakan lapis pertahanan strategis yang tidak tergantikan dalam upaya mencegah penyebaran serangan phishing di ruang digital.

Penanggulangan serangan phishing yang efektif dan berkelanjutan menuntut integrasi harmonis antara penguatan aspek manusianya (human defense) dan keandalan sistem teknisnya (technical defense). Di satu sisi, peningkatan literasi digital kritis, edukasi berbasis kurikulum, serta kesadaran kolektif menjadi fondasi utama dalam membentuk pertahanan berbasis kapasitas intelektual masyarakat guna meredam manipulasi psikologis pelaku. Di sisi lain, pembentukan benteng infrastruktur teknis mulai dari penerapan kecerdasan buatan untuk deteksi otomatis, penguatan protokol otentikasi, hingga mekanis takedown situs tiruan secara real-time menjadi lapis perlindungan mutlak untuk mempersempit celah eksploitasi siber. Sinergi holistik antara sektor publik, swasta, dan masyarakat dalam mengombinasikan kewaspadaan perilaku serta keandalan teknologi inilah yang menjadi kunci utama dalam mewujudkan ekosistem digital nasional yang aman, tangguh, dan terproteksi dari kejahatan phishing

## DAFTAR PUSTAKA

Alazab, Ammar, Jemal Abawajy, Michael Hobbs, Robert Layton, and Ansam Khraisat. "Crime Toolkits: The Productisation of Cybercrime." In *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*, 1626–32, 2013. https://doi.org/10.1109/TrustCom.2013.273.

Arachchilage, Nalin Asanka Gamagedara, and Steve Love. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective." *Computers in Human Behavior* 38 (September 2014): 304–12. https://doi.org/10.1016/j.chb.2014.05.046.

Bahari, Freyha A, Tadzmera A Daud;, Mhesi D Arabbi, Noralyn I Jalah, Nuralyn O Adjid, Fatmahal Abah, Sitti Aiman, et al. "The Psychology of Phishing: Why Users Fall Victim to Deceptive Emails." *International Journal of Innovative Science and Research Technology* 9, no. 12 (2024): 10–12.

Belton, Ian K., and Mandeep K. Dhami. "The Role of Character-Based Personal Mitigation in Sentencing Judgments." *Journal of Empirical Legal Studies* 21, no. 1 (2024): 208–39. https://doi.org/10.1111/jels.12376.

Darmawan, Irwan, Siti Ririn Sutarsih, Ulfatul Hasanah, Riyan, and Alfin Firdaus. "Analisis Pharming Dalam Cyber Crime Di Layanan Mobile Banking." *Jurnal Informasi Dan Teknologi* 5, no. 2 (2023): 159–63. https://doi.org/10.37034/jidt.v5i2.362.

Daudi, Morice. "Exploiting Human Trust in Cybersecurity: Which Trust Development Process Is Predominant in Phishing Attacks?" *Applied Cybersecurity and Internet Governance* 3, no. 2 (2024): 233–49. https://doi.org/10.60097/ACIG/199452.

Deswal, Sahil. "Critical Analysis of Laws Related to Money Laundering and Its Prevention." *RESEARCH REVIEW International Journal of Multidisciplinary* 10, no. 5 (2025): 335–42. https://doi.org/10.31305/rrijm.2025.v10.n5.037.

Dwi, Hananta. "Aggravating And Mitigating Circumstances Consideration On Sentencing." *Jurnal Hukum Dan Peradilan* 7, no. 1 (2018): 87.

Elda, Tresia. "TINJAUAN PROSES BEBAN PEMBUKTIAN TINDAK PIDANA MONEY LAUNDERING DI INDONESIA." *ADIL: Jurnal Hukum* 15, no. 1 (July 2024): 127–49. https://doi.org/10.33476/ajl.v15i1.4558.

Elsera, Riyanda. "KEBIJAKAN HUKUM PIDANA DALAM PEMBERANTASAN TINDAK PIDANA PENCUCIAN UANG DI INDONESIA." *Journal Equitable* 5 (2020). https://doi.org/https://doi.org/10.37859/jeq.v5i1.2464.

Eltaybani, Sameh. "Twenty Red Flags To Spot Phishing Emails from Predatory Journals." *Journal of Academic Ethics* 24, no. 1 (March 2026): 9. https://doi.org/10.1007/s10805-025-09679-z.

Fauzia Rahawarin, Syah Awaluddin, Ridwan Fauzi Lestaluhu, Nur Patima Sangadji, Astriyanti La Uma, Zulhairin Ode Yoni, and Ade Riski Rumain. "Analisis Yuridis Pengurangan Hukuman Oleh Hakim Mahkamah Agung Dalam Perkara Tindak Pidana Korupsi Di Indonesia." *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 1 (2024): 423–35. https://doi.org/10.55606/jhpis.v3i1.4867.

Febrika Ardy, Lutfi Aziz, Iklima Istiqomah, Angga Eben Ezer, and Shelvie Nidya Neyman. "Phishing Di Era Media Sosial: Identifikasi Dan Pencegahan Ancaman Di Platform Sosial." *Journal of Internet and Software Engineering* 1, no. 4 (June 2024): 11. https://doi.org/10.47134/pjise.v1i4.2753.

Fitaria Bantara, Margareta Theodora Simatupang, Mera Terangta, Nicholine Nicholine, and Reyane Dolimariz Putri Behuku. "Analisis Kriminologi Atas Kejahatan Dunia Maya Phising Di Era Pandemi Covid-19." *Birokrasi: JURNAL ILMU HUKUM DAN TATA NEGARA* 3, no. 1 (March 2025): 10–20. https://doi.org/10.55606/birokrasi.v3i1.1801.

Fuadi, Gumilang, Windy Virdinia Putri, and Trisno Raharjo. "Tinjauan Perampasan Aset Dalam Tindak Pidana Pencucian Uang Dari Perspektif Keadilan." *Jurnal Penegakan Hukum Dan Keadilan* 5, no. 1 (March 2024): 53–68. https://doi.org/10.18196/jphk.v5i1.19163.

Gorbunova, Larisa V., Ruslan V. Makarov, and Sergei A. Matveev. "Aggravating Circumstances. Significance and Correlation with Qualifying Signs." *Mediterranean Journal of Social Sciences* 6, no. 3 (2015): 169–78. https://doi.org/10.5901/mjss.2015.v6n3s7p169.

Holt, Thomas J., Joshua D. Freilich, and Steven M. Chermak. "Exploring the Subculture of Ideologically Motivated Cyber-Attackers." *Journal of Contemporary Criminal Justice* 33, no. 3 (August 2017): 212–33. https://doi.org/10.1177/1043986217699100.

Iqbal, Ahmad. "Merasionalkan Keadaan Yang Meringankan Pada Putusan Hakim Di Indonesia." *Jurnal Media Hukum* 13, no. 2 (2025): 303–13. https://doi.org/10.59414/jmh.v13i2.1048.

Jaya, Arizon Mega. "Implementasi Perampasan Harta Kekayaan Pelaku Tindak Pidana Korupsi (Implementation of Asset Deprivation of Criminal Act of Corruption)." *Cepalo* 1, no. 1 (2017): 19–28. https://doi.org/10.25041/cepalo.v1no1.1752.

Jones, Helen S., John N. Towse, Nicholas Race, and Timothy Harrison. "Email Fraud: The Search for Psychological Predictors of Susceptibility." *PLoS ONE* 14, no. 1 (2019): 1–15. https://doi.org/10.1371/journal.pone.0209684.

Kool, Hannah Maartje, Asier Moneva, and Rutger Leukfeldt. "Exploring Trust Signals and Pathways on Cybercrime-as-a-Service Markets: The Case of Remote Access Trojans." *Trends in Organized Crime*, July 2026. https://doi.org/10.1007/s12117-026-09606-7.

Lasmadi, Sahuri, and Elly Sudarti. "PEMBUKTIAN TERBALIK PADA TINDAK PIDANA PENCUCIAN UANG." *Refleksi Hukum: Jurnal Ilmu Hukum* 5, no. 2 (April 2021): 199–218. https://doi.org/10.24246/jrh.2021.v5.i2.p199-218.

Lastdrager, Elmer E.H. "Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature." *Crime Science* 3, no. 1 (2014): 1–10. https://doi.org/10.1186/s40163-014-0009-y.

Lee, Woonghee, Junbeom Hur, and Doowon Kim. *Beneath the Phishing Scripts: A Script-Level Analysis of Phishing Kits and Their Impact on Real-World Phishing Websites*. *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. Vol. 1. Association for Computing Machinery, 2024. https://doi.org/10.1145/3634737.3657013.

Lemay, David J., Ram B. Basnet, and Tenzin Doleck. "Examining the Relationship between Threat and Coping Appraisal in Phishing Detection among College Students." *Journal of Internet Services and Information Security* 10, no. 1 (2020): 38–49. https://doi.org/10.22667/JISIS.2020.02.29.038.

Lengkong, Lonna Yohanes. "Urgensi Penerapan Perampasan Aset Dalam Tindak Pidana Pencucian Uang." *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 3 (December 2023): 351–64. https://doi.org/10.55809/tora.v9i3.278.

Li, Yukun, Zhenguo Yang, Xu Chen, Huaping Yuan, and Wenyin Liu. "A Stacking Model Using URL and HTML Features for Phishing Webpage Detection." *Future Generation Computer Systems* 94 (May 2019): 27–39. https://doi.org/10.1016/j.future.2018.11.004.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 19–24. https://doi.org/10.18196/ijclc.v5i1.19853.

Lu, Xuecong, Jinglu Jiang, Milena Head, and Junyi Yang. "Phishing Detection in Multitasking Contexts: The Impact of Working Memory Load, Goal Activation, and Message Framing Cue on Detection Performance." *European Journal of Information Systems* 35, no. 1 (January 2026): 134–64. https://doi.org/10.1080/0960085X.2025.2548543.

Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal Usm Law Review* 6, no. 1 (2023): 226–41. https://doi.org/10.26623/julr.v6i1.6649.

Mushlihudin, Mushlihudin, and Agil Nofiyan. "Analisis Forensik Pada Web Phishing Menggunakan Metode National Institute of Standards and Technology." *Cybernetics* 4, no. 02 (2021): 11–23. https://doi.org/10.29406/cbn.v4i02.2287.

Nadia Wulandari Rotty, Anggita Cahyani, Daffa Khalisha Nabila, Rachmah Fidiastuti, and Regentio Candrika Komala Dewa. "Pemanfaatan Cryptocurrency Dalam Tindak Pidana Pencucian Uang." *Jurnal Hukum Statuta* 1, no. 2 (April 2022): 137–52. https://doi.org/10.35586/jhs.v1i2.8588.

Nailah + S, and Rosnelly + R. "Analisis Ancaman PhishingDi PlatformMedia Sosial Emailmenggunakan Metode Digital Forensic Research Workshop." *Rekayasa Sistem* 3, no. 2 (2025): 450–61.

Naqbi, Shaikha Ali Al, Haitham Nobanee, and Nejla Ould Daoud Ellili. "Global Trends and Insights into Cryptocurrency-Related Financial Crime." *Research in International Business and Finance* 75 (March 2025): 102756. https://doi.org/10.1016/j.ribaf.2025.102756.

Naresh Kamble & Nilamadhab Mishra. "Hybrid Optimization Enabled Squeeze Net for Phishing Attack Detection." *Computers & Security* 144 (2024). https://doi.org/https://doi.org/10.1016/j.cose.2024.103901.

Norma, Antara, Kesusilaan Dan, H A K Privasi, Faculty Of Law, and Dirgantara Marsekal. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Phising Di Indonesia (Studi Kasus Putusan Pengadilan Negeri Banjarbaru No 85/Pid.Sus/2022/PN Bjb)." *Jurnal Hukum Pidana, Kriminologi Dan Viktimologi* 1, no. 2 (2024): 62–78.

Nurdin, Aulia Anjani, Axara Alejendra Anjani, and Fiqih Dien Alamsyah. "Media Hukum Indonesia ( MHI ) Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi Media Hukum Indonesia ( MHI )" 2, no. 2 (2024): 74–82. https://doi.org/https://doi.org/10.5281/zenodo.11183088.

Nurfahda Annasyanda; Yardi, Nayottama Aryasuta; Deni, Fitra, Amanda Faizah; Jelita Putri. "ANALISIS PENIPUAN ONLINE DALAM BENTUK PHISING MENURUT PERSPEKTIF HUKUM INDONESIA." *SAHID BANKING JOURNAL*, no. Vol 4 No 1 (2024): OKTOBER 2024 (2024): 50–57. https://doi.org/10.56406/sahidbankingjournal.v4i1.193.

Onwuadiamu, Gift. "Cybercrime in Criminology; A Systematic Review of Criminological Theories, Methods, and Concepts." *Journal of Economic Criminology* 8, no. December 2024 (2025): 100136. https://doi.org/10.1016/j.jeconc.2025.100136.

Oroni, Chrispus Zacharia, and Fu Xianping. "Evaluating the Influence of Cybersecurity Policies and Cybersecurity Behavior on Institutional Security Performance in Remote Learning: The Moderating Role of Technological Readiness." *Sustainable Futures* 10 (December 2025): 101554. https://doi.org/10.1016/j.sftr.2025.101554.

PSHK. "Penjelasan Hukum Tentang Perampasan Aset Tanpa Pemidanaan." *PSHK Restatement*, 2019.

Puanandini, Dewi Asri. "PIDANA PENCUCIAN UANG HASIL KEJAHATAN SIBER (CYBER CRIME) MELALUI MATA UANG DIGITAL (CRYPTO CURRENCY)." *JURNAL PEMULIAAN HUKUM* 4, no. 2 (October 2021): 57–70. https://doi.org/10.30999/jph.v4i2.1480.

Putri, Dina. "Penerapan Perampasan Aset Sebagai Tambahan Dalam Tindak Pidana Korupsi Indonesia." *Jurnal Hukum Samudra Keadilan* 19, no. 2 (2024): 302–19.

Putri Ramadhani Rangkuti, Muhammad Aldi Khoiri, Sumantri Ritonga, and Putri Nabila Sitorus Pane. "Sanksi Pidana Terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia." *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi* 2, no. 3 (2025): 291–305. https://doi.org/10.62383/konstitusi.v2i3.908.

Rahman, Rahmat Eka Putra R Palaloi. Rakhmadi. "ANALISIS DAN PENCEGAHAN SERANGAN SOSIAL ENGINERING PADA JARINGAN KOMPUTER STUDI KASUS PENIPUAN INVESTASI CRYPTO." *Jurnal Riset Sistem Informasi* 1, no. 3 (2024). https://doi.org/https://doi.org/10.69714/8b7xtv35.

Ribeiro, Liliana, Inês Sousa Guedes, and Carla Sofia Cardoso. "Which Factors Predict Susceptibility to Phishing? An Empirical Study." *Computers & Security* 136 (January 2024): 103558. https://doi.org/10.1016/j.cose.2023.103558.

Richa Goenka, Meenu Chawla & Namita Tiwari. "A Comprehensive Survey of Phishing: Mediums, Intended Targets, Attack and Defence Techniques and a Novel Taxonomy." *International Journal of Information Security* 23 (2024): 819–48. https://doi.org/https://doi.org/10.1007/s10207-023-00768-x.

Romagna, Marco, and Rutger E. Leukfeldt. "Becoming a Hacktivist. Examining the Motivations and the Processes That Prompt an Individual to Engage in Hacktivism." *Journal of Crime and Justice* 47, no. 4 (August 2024): 511–29. https://doi.org/10.1080/0735648X.2023.2216189.

Sahfitri, Afifah, and Rosmalinda Rosmalinda. "Penipuan Digital Melalui Tautan Phishing." *Jurnal Dialektika Hukum* 6, no. 2 (2024): 92–107. https://doi.org/10.36859/jdh.v6i2.2881.

Saidah, Indah Siti. "Keamanan Digital Dalam Perspektif Al-Qur'an: Kasus Kejahatan Phishing." *Mashadiruna Jurnal Ilmu Al-Qur'an Dan Tafsir* 3, no. 2 (October 2024): 109–14. https://doi.org/10.15575/mjiat.v3i2.34819.

Sarno, Dawn M., Maggie W. Harris, and Jeffrey Black. "Which Phish Is Captured in the Net? Understanding Phishing Susceptibility and Individual Differences." *Applied Cognitive Psychology* 37, no. 4 (July 2023): 789–803. https://doi.org/10.1002/acp.4075.

Sembiring, Patricia Edina. "Menilai Pemberlakuan Pembuktian Terbalik Pada Tindak Pidana Pencucian Uang Sebagai Kejahatan Proxy Di Dalam Aset Kripto." *Integritas : Jurnal Antikorupsi*, June 2024. https://doi.org/10.32697/integritas.v10i1.1033.

Shiva, Khadizah Aliyah, Salsabila Afifany Susanta Putry, and Asmak UI Hosnah. "Kebijakan Penegakan Hukum Tindak Pidana Terhadap Pencucian Uang (Money Laundering) Di Indonesia." *TATOHI: Jurnal Ilmu Hukum* 4, no. 10 (2024): 803. https://doi.org/10.47268/tatohi.v4i10.2581.

Sutanto, Jason Matthew, and Nadia Nadia. "Cyber Security Awareness Simulation for Web Phishing in E-Commerce." *Engineering, MAthematics and Computer Science Journal (EMACS)* 7, no. 1 (January 2025): 69–78. https://doi.org/10.21512/emacsjournal.v7i1.12100.

Swarnalatha, KC. Ramchandra, KC. Anshari, Kaushar. Ojha, Love. Sharma, Sanjok Subedi. "Real-Time Threat Intelligence-Block Phising Attacks." *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2021. https://doi.org/10.1109/CSITSS54238.2021.9683237.

Wicaksono, O S, and S Mahmudah. "Analisis Hukum Cryptocurrency Sebagai Alat Pembayaran Di Indonesia: Perspektif Yuridis." *Jurnal Preferensi Hukum* 4, no. 2 (2023): 202–19. https://doi.org/https://doi.org/10.55637/jph.4.2.7147.202-219.

Yusuf, Mohammad, and Maysarah. "Penerapan Hukum Terhadap Pelaku Kejahatan Tindak Pidana Akses Illegal." *Jurnal Pendidikan Dan Konseling* 4 (2022): 9735–40. https://doi.org/https://doi.org/10.31004/jpdk.v4i6.9920.

Zhao, Rui, Samantha John, Stacy Karas, Cara Bussell, Jennifer Roberts, Daniel Six, Brandon Gavett, and Chuan Yue. "Design and Evaluation of the Highly Insidious Extreme Phishing Attacks." *Computers & Security* 70 (September 2017): 634–47. https://doi.org/10.1016/j.cose.2017.08.008.