

Penipuan Top Up Robux via Login: Analisis Modus Operandi, Kerentanan Korban, dan Strategi Pencegahannya

Ibnu Atiiq Ash Shiddiq^{1*}, Mohammad Fahmi Miftah²

¹Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia, E-mail: 23071010009@student.upnjatim.ac.id

²Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia, E-mail: 23071010034@student.upnjatim.ac.id

Abstract

This study examines the increasing number of Robux top-up frauds targeting users aged children and adolescents through structured social engineering strategies. Perpetrators typically create fake identities on social media, offer significantly lower top-up prices, and create a false sense of urgency and trust to encourage victims to hand over login credentials. Once the account is compromised, the perpetrators drain the Robux, remove valuable items, and even sell the account. This phenomenon reveals weak digital literacy, minimal parental supervision, and suboptimal platform protection for young users. Using a qualitative approach based on literature studies, this study emphasizes the need for digital literacy education, strengthened platform security, and legal policies that are more responsive to the dynamics of cybercrime in the online gaming ecosystem.

Keywords: Digital Fraud; Robux; Social Engineering; Children And Teens; Cybersecurity; Online Gaming.

Abstrak

Penelitian ini mengkaji modus penipuan top up Robux melalui login yang semakin meningkat dan menasar pengguna berusia anak hingga remaja melalui strategi rekayasa sosial yang terstruktur. Pelaku biasanya membangun identitas palsu di media sosial, menawarkan harga top up jauh lebih murah, serta menciptakan urgensi dan kepercayaan palsu untuk mendorong korban menyerahkan data login. Setelah akun dikuasai, pelaku mengurus Robux, memindahkan item berharga, hingga menjual akun korban. Fenomena ini mengungkap lemahnya literasi digital, minimnya pengawasan orang tua, serta kurang optimalnya perlindungan platform terhadap pengguna muda. Dengan pendekatan kualitatif berbasis studi literatur, penelitian ini menegaskan perlunya pendidikan literasi digital, penguatan keamanan platform, dan kebijakan hukum yang lebih responsif terhadap dinamika kejahatan siber dalam ekosistem permainan daring.

Kata Kunci: Penipuan Digital; Robux; Rekayasa Sosial; Anak Dan Remaja; Keamanan Siber; Permainan Daring.

I. Pendahuluan

Penipuan top up Robux via login modus penipuan yang meminta korban memberikan akses dengan username dan kata sandi telah meningkat dalam beberapa tahun terakhir. Pelaku berhasil membuat korban merasa aman dan kredibel dengan menggunakan iklan murah, promosi palsu, dan menyamar sebagai penjual resmi. Prakteknya, pelaku meminta korban untuk mengakses situs web yang mirip dengan situs web resmi Roblox atau meminta informasi login akun pribadi mereka. Setelah mendapatkan akses, pelaku dapat mengambil alih akun, mengurus Robux korban, memindahkan barang berharga, atau bahkan menjual akun kepada pihak lain. Modus ini berkembang menjadi salah satu jenis social engineering yang memanfaatkan kurangnya literasi digital, kecenderungan ekstrim pengguna muda, dan kurangnya pengawasan orang tua..

Meningkatnya jumlah kasus penipuan jenis ini menunjukkan bahwa ada masalah hukum dan sosial yang penting yang perlu diteliti secara menyeluruh. Penipuan digital ini diatur

oleh ketentuan pidana dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Ketentuan-ketentuan ini terutama berkaitan dengan akses ilegal, manipulasi data elektronik, dan penggelapan aset digital. Korban penipuan top up Robux, bagaimanapun, biasanya adalah anak-anak atau remaja yang belum memahami prosedur pelaporan, proses hukum, atau bahkan tidak tahu bahwa tindakan yang mereka alami termasuk tindak pidana siber. Ini menimbulkan pertanyaan tentang seberapa baik sistem hukum melindungi kelompok rentan tersebut dan bagaimana tanggung jawab platform mencegah kejahatan serupa.

Sebaliknya, dari sudut pandang sosiologis dan psikologis, modus penipuan ini memanfaatkan dinamika interaksi sosial dalam komunitas gim, terutama tekanan kompetitif antar pemain, keinginan untuk diakui, dan keinginan untuk mendapatkan item eksklusif. Karena perkembangan kognitif mereka yang masih dalam tahap pencarian identitas dan belum sepenuhnya mampu mempertimbangkan konsekuensi jangka panjang dari tindakan, anak-anak dan remaja adalah kelompok yang paling rentan menjadi korban. Melalui pesan seperti "promo terbatas", "diskon besar untuk hari ini saja", atau "top up tercepat hanya dengan login", pelaku memanfaatkan pola pikir ini untuk menciptakan sensasi urgensi. Banyak orang tidak tahu tentang keamanan digital atau bagaimana melakukan transaksi aman saat bermain permainan online, yang memperburuk keadaan

Selain itu, platform media sosial seperti Instagram, TikTok, dan WhatsApp memungkinkan pelaku melakukan tindakan mereka. Korban lebih mudah terkecoh dengan akun palsu dengan tampilan profesional, testimoni palsu, dan fitur highlight untuk menunjukkan bukti transaksi palsu. Sebelum akhirnya meminta data login, pelaku juga sering menggunakan fitur perpesanan pribadi untuk membangun kepercayaan dan kedekatan psikologis. Oleh karena itu, penipuan top up Robux melalui login bukan hanya masalah kriminalitas digital tetapi juga masalah komunikasi persuasif yang memanfaatkan kelemahan mental dan emosional korban. Korban terkena dampak ekonomi dan psikologis nyata dari fenomena ini. Korban dari sudut pandang ekonomi kehilangan akses ke akun yang mungkin telah dibangun selama bertahun-tahun dan juga kehilangan Robux atau item virtual bernilai tinggi. Dalam ekonomi digital kontemporer, nilai aset digital sangat penting, meskipun tidak selalu dianggap sebagai benda dalam hukum konvensional. Banyak korban mengalami trauma digital karena kehilangan akun

yang memiliki nilai sentimental, serta rasa kecewa, marah, dan malu. Bagi anak-anak, kehilangan akun permainan dapat berdampak pada suasana hati, keinginan untuk belajar, dan perilaku sehari-hari mereka..

Sebaliknya, peningkatan kasus penipuan top up Robux melalui login menunjukkan betapa pentingnya orang tua dan lembaga pendidikan mengajarkan anak-anak tentang literasi digital, privasi, dan perilaku aman saat bertransaksi di internet . Tanpa pemahaman yang cukup, anak-anak mudah percaya pada hal-hal yang tampak meyakinkan meskipun sebenarnya berbahaya. Selain itu, adalah tanggung jawab platform Roblox untuk meningkatkan sistem keamanan, memperketat proses verifikasi, dan membuat kanal pelaporan yang lebih mudah digunakan oleh pengguna di bawah umur. Untuk menghindari kerugian yang lebih besar, keluarga, sekolah, pemerintah, dan platform harus bertanggung jawab satu sama lain.

Dari perspektif kebijakan publik, fenomena penipuan digital seperti ini menunjukkan kurangnya literasi dan kebijakan di tingkat mikro, terutama dalam hal mengawasi aktivitas digital harian anak. Meskipun undang-undang telah dibuat oleh pemerintah untuk melindungi data dan mencegah pelanggaran siber, implementasinya masih belum optimal. Banyak keluarga tidak tahu cara menggunakan fitur keamanan dasar seperti autentikasi dua faktor, verifikasi email, dan pengaturan privasi akun. Hal ini menunjukkan bahwa masalah terbesar tidak hanya kekurangan aturan, tetapi juga kurangnya interaksi sosial, pelatihan, dan pendampingan pengguna internet. Sangat penting untuk melakukan penelitian ini mengingat kompleksitas masalah tersebut. Studi tentang modus operandi, faktor kerentanan korban, dan teknik pencegahannya telah menambah literatur tentang kejahatan siber dalam konteks permainan daring. Selain itu, mereka menjadi rujukan praktis bagi masyarakat, penegak hukum, dan pembuat kebijakan. Intervensi preventif dapat dirancang secara lebih tepat sasaran dengan mengetahui bagaimana pelaku beroperasi dan bagaimana korban terjebak dalam situasi tersebut.

Dari perspektif kebijakan publik, fenomena penipuan digital seperti ini menunjukkan kurangnya literasi dan kebijakan di tingkat mikro, terutama dalam hal mengawasi aktivitas digital harian anak. Meskipun undang-undang telah dibuat oleh pemerintah untuk melindungi data dan mencegah pelanggaran siber, implementasinya masih belum optimal. Banyak keluarga tidak tahu cara menggunakan fitur keamanan dasar seperti

autentikasi dua faktor, verifikasi email, dan pengaturan privasi akun. Hal ini menunjukkan bahwa masalah terbesar tidak hanya kekurangan aturan, tetapi juga kurangnya interaksi sosial, pelatihan, dan pendampingan pengguna internet. Sangat penting untuk melakukan penelitian ini mengingat kompleksitas masalah tersebut. Studi tentang modus operandi, faktor kerentanan korban, dan teknik pencegahannya telah menambah literatur tentang kejahatan siber dalam konteks permainan daring. Selain itu, mereka menjadi rujukan praktis bagi masyarakat, penegak hukum, dan pembuat kebijakan. Intervensi preventif dapat dirancang secara lebih tepat sasaran dengan mengetahui bagaimana pelaku beroperasi dan bagaimana korban terjebak dalam situasi tersebut.

Selain itu, penelitian ini diharapkan akan membantu diskursus hukum siber di Indonesia, terutama mengenai perlindungan anak dalam ruang digital, peraturan yang mengatur transaksi digital di platform permainan, dan penegakan hukum terhadap pelanggaran yang berkaitan dengan aset virtual. Penipuan top up Robux melalui login tampaknya hanya masalah kecil, tetapi masalah ini terkait erat dengan perilaku ekonomi digital yang semakin kompleks dan partisipasi pengguna di bawah umur. Oleh karena itu, diperlukan pendekatan multidisipliner yang melibatkan pendidikan, teknologi informasi, psikologi, dan hukum.

II. Metode

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk menggambarkan secara mendalam pola penipuan top up Robux via login, karakteristik pelaku, serta faktor-faktor yang menyebabkan korban mudah terjerat dalam penipuan tersebut. Pendekatan ini dipilih karena fenomena penipuan digital tidak dapat dijelaskan hanya melalui angka, melainkan membutuhkan pemahaman kontekstual mengenai perilaku pelaku dan dinamika psikologis korban. Data penelitian diperoleh melalui kombinasi antara wawancara terbatas dengan beberapa korban yang pernah mengalami pencurian akun Roblox akibat memberikan data login kepada penjual top up palsu serta observasi terhadap akun-akun media sosial yang menawarkan jasa top up Robux dengan pola-pola mencurigakan. Selain itu, penelitian ini memanfaatkan sumber data sekunder seperti artikel ilmiah tentang kejahatan siber, artikel tentang rekayasa sosial, Undang-Undang Informasi dan Transaksi Elektronik, dan KUHP, serta kebijakan keamanan Roblox yang berkaitan dengan perlindungan akun dan proses top up resmi. Selanjutnya,

semua data dianalisis menggunakan teknik analisis tematik untuk menemukan kesamaan pola, tema, dan strategi yang digunakan pelaku untuk melakukan penipuan. Dengan melakukan triangulasi sederhana, informasi dari wawancara, temuan observasi, dan literatur pendukung dibandingkan untuk memperkuat validitas data. Penelitian diharapkan dapat memberikan gambaran menyeluruh tentang modus penipuan top up Robux, kerentanan korban, dan metode pencegahan yang berguna untuk mengurangi risiko penipuan serupa.

III. Hasil dan Pembahasan

A. Modus Operandi Penipuan Robux

Metode penipuan top up Robux melalui login pada dasarnya memanfaatkan kelemahan literasi digital pengguna, terutama anak-anak dan remaja, dengan menggunakan strategi rekayasa sosial yang digunakan secara berulang. Pelaku memulai aksinya dengan membangun identitas palsu di berbagai platform media sosial seperti Instagram, TikTok, dan Facebook. Identitas tersebut tidak dibuat secara acak; pelaku menggunakan logo Roblox, foto bukti transaksi palsu, dan testimoni palsu yang seolah-olah menunjukkan bahwa mereka adalah penyedia layanan top up terpercaya. Praktik ini membuat calon korban percaya bahwa akun tersebut memiliki hubungan dengan layanan top up resmi. Pelaku kemudian menawarkan paket top up Robux dengan harga jauh lebih murah daripada harga resmi di situs Roblox setelah reputasi palsu berhasil dibangun. “Promo terbatas”, “diskon hari ini saja”, atau “harga reseller” biasanya dijadikan alat persuasi. Korban yang mayoritas masih usia sekolah dasar atau menengah secara psikologis terdorong mengambil keputusan cepat tanpa melakukan verifikasi. Setelah itu pelaku meminta korban berkomunikasi melalui pesan pribadi seperti WhatsApp, Telegram, atau Direct Message untuk menciptakan rasa aman.

Pelaku kemudian memasukkan data login korban, mengganti kata sandi, alamat email pemulihan, dan menonaktifkan fitur keamanan seperti Verifikasi Dua Langkah sehingga korban kehilangan akses sepenuhnya. Robux, item langka, dan aset virtual lainnya dipindahkan atau dijual, bahkan akun yang telah diretas sering dijual kembali melalui pasar gelap akun gim daring. Pelaku lalu memutus seluruh kontak dengan korban, menghapus akun media sosial, atau membuat identitas baru untuk mengulangi modus yang sama terhadap korban lainnya. Pola ini terus berulang karena sebagian besar korban adalah anak-anak yang tidak memahami mekanisme pelaporan resmi.

Empat komponen utama yang digunakan dalam modus ini dari perspektif rekayasa sosial adalah otoritas palsu, urgensi palsu, eksploitasi ketidaktahuan, dan manipulasi emosional. Dengan demikian, penipuan top up Robux melalui login tidak hanya berupa pencurian akun digital, tetapi merupakan hasil eksploitasi psikososial yang terstruktur yang memanfaatkan lemahnya literasi digital masyarakat usia muda.

B. Karakteristik Modus Penipuan Dalam Perspektif Hukum Pidana Siber

Modus penipuan top up Robux melalui permintaan login memiliki karakteristik sebagai bentuk kejahatan siber kontemporer yang menggabungkan unsur penipuan konvensional dengan pemanfaatan sistem elektronik secara melawan hukum. Berbeda dengan peretasan murni yang menitikberatkan pada serangan teknis terhadap sistem keamanan digital, kejahatan ini justru mengeksploitasi aspek manusia sebagai titik terlemah dalam sistem keamanan (*the weakest link in cybersecurity*). Pelaku tidak perlu menembus firewall atau enkripsi sistem Roblox, melainkan cukup memanipulasi korban agar dengan sukarela menyerahkan kredensial akses akunnya. Kondisi ini menunjukkan bahwa kejahatan siber tidak selalu bergantung pada kecanggihan teknologi, tetapi lebih pada kecanggihan strategi manipulasi psikologis yang terstruktur dan berulang.

Karakteristik utama dari modus penipuan ini adalah sifatnya yang anonim, tidak terbatas wilayah, dan sulit ditelusuri secara yuridis. Media sosial, aplikasi pesan instan, serta sistem pembayaran digital memungkinkan pelaku beroperasi secara lintas daerah bahkan lintas negara tanpa harus menampilkan identitas asli. Dalam praktiknya, pelaku menggunakan akun palsu, nomor telepon prabayar yang mudah diganti, serta jaringan internet yang tidak mudah dilacak. Keadaan ini menimbulkan hambatan serius bagi aparat penegak hukum dalam melakukan penyelidikan dan pembuktian, karena alat bukti digital sering kali terbatas, mudah dihapus, dan melibatkan yurisdiksi yang berbeda. Dengan demikian, penipuan top up Robux via login termasuk dalam kategori kejahatan siber yang berisiko tinggi lolos dari penegakan hukum konvensional.

Penggunaan identitas palsu sebagai instrumen utama penipuan menjadi karakteristik yang tidak terpisahkan dari modus ini. Pelaku secara sadar membentuk persona digital dengan tampilan profesional, lengkap dengan logo Roblox, testimoni palsu, serta tangkapan layar bukti transaksi yang telah dimanipulasi. Identitas semu ini berfungsi untuk menciptakan kesan kredibel di mata calon korban, terutama anak-anak yang belum memiliki kemampuan verifikasi informasi secara kritis. Dalam perspektif hukum

pidana siber, praktik ini menunjukkan adanya penyalahgunaan sistem elektronik sebagai sarana kejahatan, di mana teknologi informasi tidak hanya menjadi alat pendukung, tetapi juga menjadi medium utama terjadinya delik.

Karakteristik berikutnya adalah obyek kejahatan yang berupa aset digital bernilai ekonomi, yaitu Robux dan item virtual dalam akun Roblox. Dalam perkembangan ekonomi digital modern, aset virtual tidak lagi dipandang sebagai sekadar objek permainan, melainkan telah mengalami komodifikasi menjadi barang bernilai tukar. Robux dapat dibeli dengan uang riil, diperdagangkan di pasar sekunder, serta digunakan untuk memperoleh keuntungan ekonomi. Oleh karena itu, penguasaan Robux secara melawan hukum melalui pengambilalihan akun korban telah memenuhi unsur perampasan kekayaan dalam pengertian hukum pidana modern. Dengan demikian, kerugian korban tidak bersifat abstrak, tetapi nyata dan terukur secara ekonomi.

Karakteristik yang memperberat pertanggungjawaban pidana dalam modus ini adalah status korban yang dominan merupakan anak di bawah umur. Anak sebagai subjek hukum memiliki keterbatasan dalam memahami risiko transaksi digital, serta rentan terhadap manipulasi psikologis. Kejahatan yang menasar anak tidak hanya melanggar norma pidana umum, tetapi juga bertentangan dengan prinsip perlindungan anak dalam hukum nasional dan internasional. Oleh karena itu, penipuan top up Robux via login tidak hanya berdimensi “kejahatan terhadap harta benda”, tetapi juga mengandung unsur eksploitasi terhadap kerentanan anak di ruang digital.

Apabila ditinjau dari perspektif hukum positif di Indonesia, perbuatan pelaku telah memenuhi unsur Pasal 378 KUHP tentang penipuan, karena dilakukan dengan tipu muslihat dan rangkaian kebohongan untuk menguasai harta milik orang lain. Selain itu, pelaku juga melanggar Pasal 30 ayat (1), (2), dan (3) UU ITE, karena melakukan akses tanpa hak terhadap sistem elektronik milik korban, yang sanksinya diatur dalam Pasal 46 UU ITE. Oleh sebab itu, penegakan hukum terhadap modus penipuan ini secara normatif dapat diterapkan secara kumulatif, yakni melalui KUHP dan UU ITE sekaligus.

C. Strategi Pencegahan Penipuan Top Up Robux via Login

Strategi pencegahan terhadap penipuan top up Robux melalui permintaan login tidak dapat dilakukan secara parsial atau hanya dibebankan pada satu pihak tertentu, melainkan harus ditempatkan dalam kerangka pendekatan sistemik dan multidisipliner

yang melibatkan negara, platform digital, keluarga, lembaga pendidikan, serta pengguna itu sendiri. Kejahatan siber jenis ini merupakan produk dari interaksi antara teknologi, kelemahan manusia, serta ketidaksiapan sistem hukum dan sosial dalam merespons dinamika ruang digital. Oleh karena itu, upaya pencegahan yang efektif harus diarahkan tidak hanya pada aspek represif (penindakan hukum), tetapi juga pada aspek preventif dan edukatif yang berorientasi jangka panjang. Pencegahan tidak cukup dimaknai sebagai upaya mengurangi jumlah korban, tetapi juga sebagai proses membangun ekosistem digital yang aman, beretika, dan berkeadaban.

Dari perspektif negara dan kebijakan publik, strategi pencegahan harus diwujudkan melalui penguatan regulasi dan optimalisasi peran institusi penegak hukum di bidang siber. Meskipun Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai instrumen hukum utama dalam penanggulangan kejahatan siber, namun pada tataran implementasi masih ditemukan berbagai kendala, seperti keterbatasan sumber daya penyidik siber, lemahnya koordinasi lintas lembaga, serta rendahnya tingkat pelaporan masyarakat. Negara perlu membentuk kebijakan yang lebih progresif, misalnya melalui penguatan unit khusus kejahatan siber yang terfokus pada perlindungan anak di ruang digital, peningkatan kapasitas forensik digital, serta kerja sama internasional untuk menelusuri pelaku yang beroperasi lintas negara. Tanpa dukungan negara yang kuat dan responsif, penindakan terhadap penipuan top up Robux akan selalu tertinggal dibandingkan dengan kecepatan inovasi modus kejahatan itu sendiri.

Selain negara, peran platform digital dalam hal ini Roblox dan penyedia media sosial memiliki posisi yang sangat strategis dalam upaya pencegahan. Platform tidak dapat lagi hanya menempatkan dirinya sebagai penyedia layanan netral (neutral service provider), tetapi harus memikul tanggung jawab moral dan sosial sebagai pengelola ruang publik digital. Bentuk pencegahan yang dapat dilakukan antara lain adalah penguatan sistem keamanan akun melalui verifikasi berlapis, pembatasan interaksi akun baru dengan pengguna anak, serta deteksi otomatis terhadap aktivitas mencurigakan seperti pesan massal berisi penawaran top up ilegal. Selain itu, platform juga wajib menyediakan mekanisme pengaduan yang cepat, mudah, dan berpihak pada korban anak. Ketika platform bersikap pasif dan hanya reaktif setelah terjadi kejahatan, maka sesungguhnya

platform telah turut berkontribusi dalam membiarkan ruang digital menjadi ladang subur bagi praktik kejahatan siber.

Strategi pencegahan yang tidak kalah penting adalah penguatan peran keluarga, khususnya orang tua, sebagai garda terdepan perlindungan anak di ruang digital. Anak-anak sebagai pengguna utama Roblox belum memiliki kapasitas penuh untuk membedakan antara interaksi yang aman dan yang berbahaya. Oleh karena itu, orang tua tidak cukup hanya membekali anak dengan perangkat digital, tetapi juga harus membekali mereka dengan literasi keamanan digital. Pengawasan tidak harus selalu bersifat represif atau membatasi secara kaku, tetapi dapat diwujudkan dalam bentuk pendampingan, dialog terbuka, serta edukasi tentang risiko-risiko yang ada di dunia maya. Orang tua perlu memahami bagaimana mekanisme top up, bagaimana pola penipuan bekerja, serta bagaimana mengenali tanda-tanda awal kejahatan digital. Tanpa keterlibatan aktif keluarga, anak akan tetap berada dalam posisi yang sangat rentan terhadap manipulasi pelaku.

Lembaga pendidikan juga memegang peran strategis dalam membangun ketahanan digital (digital resilience) pada anak dan remaja. Sekolah tidak lagi cukup hanya berfokus pada penguasaan teknologi dari aspek keterampilan teknis, tetapi juga harus mengintegrasikan pendidikan etika digital, keamanan siber, dan perlindungan data pribadi dalam kurikulum. Anak harus diajarkan sejak dini bahwa identitas digital, kata sandi, kode OTP, dan data pribadi merupakan bagian dari hak privat yang tidak boleh diserahkan kepada siapa pun. Pendidikan semacam ini tidak boleh bersifat insidental, melainkan harus menjadi bagian dari proses pembelajaran yang berkesinambungan. Dengan demikian, pencegahan penipuan tidak hanya bersandar pada larangan semata, tetapi pada pembentukan kesadaran kritis siswa sebagai warga digital (digital citizen).

Dari sudut pandang pengguna, khususnya anak dan remaja, pencegahan menuntut adanya transformasi pola pikir dari budaya digital yang serba instan menuju budaya digital yang berorientasi pada keamanan dan kehati-hatian. Anak perlu dibangun kesadarannya bahwa tidak ada keuntungan cepat tanpa risiko, serta tidak ada layanan resmi yang meminta kata sandi atau kode OTP. Pencegahan pada level individu dapat dilakukan melalui kebiasaan-kebiasaan sederhana, seperti menggunakan kata sandi yang kuat, mengaktifkan verifikasi dua langkah, tidak mudah percaya pada akun asing, serta selalu melakukan verifikasi terhadap setiap penawaran yang menggiurkan. Kesadaran ini

harus dibangun secara bertahap melalui pengalaman, edukasi, dan contoh yang konsisten dari lingkungan sekitar.

Lebih jauh, pencegahan penipuan top up Robux juga harus ditempatkan dalam kerangka perlindungan anak dalam ruang siber yang berbasis hak asasi manusia. Anak memiliki hak untuk memperoleh rasa aman di ruang digital sebagaimana di ruang fisik. Ketika negara, platform, keluarga, dan masyarakat gagal membangun sistem perlindungan yang memadai, maka anak akan terus menjadi korban dari eksploitasi ekonomi digital yang terselubung. Oleh karena itu, strategi pencegahan tidak boleh bersifat reaktif dan sesaat, tetapi harus dirancang sebagai kebijakan jangka panjang yang terintegrasi, berkelanjutan, dan berbasis pada kepentingan terbaik bagi anak (the best interest of the child).

Secara kritis dapat dinyatakan bahwa selama ini pendekatan pencegahan terhadap kejahatan siber yang menyasar anak masih cenderung bersifat normatif dan simbolik, melalui imbauan-imbauan umum tanpa disertai mekanisme kontrol yang efektif. Edukasi sering dilakukan secara seremonial, sementara pengawasan nyata masih lemah. Di sisi lain, penegakan hukum sering kali baru bergerak setelah korban mengalami kerugian besar, sehingga fungsi preventif hukum menjadi tidak optimal. Oleh karena itu, diperlukan perubahan paradigma dari penanggulangan yang berbasis reaksi menjadi pencegahan yang berbasis sistem dan kesadaran kolektif.

IV. Kesimpulan

Penipuan top up Robux melalui permintaan login merupakan bentuk kejahatan siber berbasis rekayasa sosial (social engineering) yang menitikberatkan pada manipulasi psikologis korban, bukan pada pembobolan sistem teknologi. Modus ini dijalankan secara terstruktur melalui tahapan pencarian target, pembentukan kepercayaan semu, pengambilalihan akun, hingga eksploitasi aset digital. Anak-anak dan remaja menjadi kelompok yang paling rentan karena secara psikologis masih berada pada fase perkembangan emosi dan pengambilan keputusan yang belum matang, serta didukung oleh rendahnya literasi keamanan digital. Dalam konteks ini, Robux dan item virtual tidak lagi dapat dipandang sekadar sebagai elemen permainan, melainkan telah bertransformasi menjadi aset digital bernilai ekonomi yang rawan menjadi objek kejahatan.

Dari perspektif hukum pidana penipuan top up Robux via login secara yuridis telah memenuhi unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP, serta tindak pidana akses ilegal terhadap sistem elektronik berdasarkan Pasal 30 jo. Pasal 46 UU ITE. Selain itu, dominannya korban anak menjadikan kejahatan ini juga bersinggungan dengan rezim perlindungan anak, yang mewajibkan negara memberikan perlindungan khusus terhadap anak di ruang digital. Namun demikian, dalam praktiknya, masih terdapat kesenjangan antara norma hukum dan efektivitas perlindungan bagi korban, baik karena keterbatasan pelaporan, rendahnya kesadaran hukum masyarakat, maupun kompleksitas pembuktian dalam kejahatan siber yang bersifat anonim dan lintas wilayah.

Kerentanan korban dalam kasus ini dipengaruhi oleh rendahnya literasi digital, lemahnya pengawasan orang tua, kurang optimalnya peran sekolah dalam pendidikan keamanan siber, serta budaya transaksi digital yang serba instan dan berorientasi pada keuntungan cepat. Dampak yang ditimbulkan pun tidak terbatas pada kerugian ekonomi, tetapi juga mencakup tekanan psikologis, trauma digital, serta gangguan terhadap relasi sosial korban, khususnya anak. Oleh karena itu, pencegahan penipuan top up Robux tidak dapat dilakukan secara parsial, melainkan harus ditempuh melalui pendekatan yang komprehensif dan sinergis antara negara, platform digital, keluarga, lembaga pendidikan, dan masyarakat. Hanya dengan kolaborasi seluruh unsur tersebut ekosistem permainan daring dapat dibangun secara lebih aman, beretika, dan berorientasi pada perlindungan pengguna, khususnya anak sebagai kelompok paling rentan.

Ucapan Terimakasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada dosen pembimbing, Bapak Eka Nanda Ravizki S.H., LL.M.. atas bimbingan dan dukungannya selama proses pembuatan jurnal ini. Penulis juga menyampaikan apresiasi yang mendalam kepada Komunitas Riset Mahasiswa Fakultas Hukum UPN "Veteran" Jawa Timur yang telah menyediakan fasilitas, wadah kolaborasi, dan kesempatan untuk mewujudkan karya ilmiah ini. Tidak lupa, penghargaan tulus disampaikan kepada kami sendiri, Jens Thomos Gratya Sinaga dan Deyna Keysha yang telah mendedikasikan waktu, usaha, dan komitmen untuk menyelesaikan jurnal ini dengan baik.

Referensi

- Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, 5(02), 7.
- Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum*, 5(2), 55–63.
- Albladi, S., & Weir, G. (2020). Predicting Victims of Social Engineering Attacks: A Systematic Literature Review. *Computers & Security*, 90(1), 101710.
- ANTARA. (2025, August 16). Cara menghindari penipuan dan scam di game Roblox. *Antaranews.com*.
- Ariyanto, D. (2020). Faktor penyebab kerentanan remaja terhadap kejahatan siber: Sebuah tinjauan psikososial. *Jurnal Kriminologi Indonesia*, 16(2), 145–158.
- Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi pencegahan kejahatan siber di Indonesia: Sinergi antara UU ITE dan kebijakan keamanan digital. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(2), 3614–3625.
- Fadilah, A. (2022). Teknik Persuasi dalam Modus Penipuan Online. *Jurnal Komunikasi Digital*.
- Hendrik S, A. (2019). Modus operandi dan problematika penanggulangan tindak pidana penipuan daring. *Mimbar Hukum*, 31(1), 59–74.
- Hidayat, R., & Satriani, R. (2021). Pola penipuan online berbasis media sosial dan karakteristik korbannya. *Jurnal Hukum & Teknologi*, 5(1), 33–47.
- <https://www.antaranews.com/berita/5042905/cara-menghindari-penipuan-danscamdi-gameroblox>
- Livingstone, S., & Byrne, J. (2023). Children's Digital Safety: Risks, Resilience, and Policy Challenges. *Journal of Children and Media*, 17(2), 147.
- Nandakumar, K., et al. (2021). Understanding Online Fraud Victimization Among Adolescents. *Journal of Cybersecurity*, 7(1), 3.
- Nugroho, R. A. (2023). Perdagangan Akun Gim dan Risiko Kejahatan Siber. *Jurnal Keamanan Siber*.
- Pramudita, K. (2023). Identitas Palsu dalam Penipuan Siber pada Platform Media Sosial. *Jurnal Teknologi Informasi*.
- Pratama, A. B. (2022). Digital scam and youth vulnerability: An empirical study on online gaming communities. *International Journal of Cyber Behavior Studies*, 4(3), 112–128.

- Putri, N. A. (2024). Kerentanan Anak dalam Penipuan Digital dan Literasi Siber. *Jurnal Pendidikan dan Teknologi*.
- Rahmadani, N. R., Amelia, R., Putri, S. A., Ramadhannia, R. N., Putra, R. M., Pratiwi, M. G., et al. (2025). Tinjauan yuridis tanggung jawab orang tua dalam pencegahan kejahatan siber terhadap anak di bawah umur dalam penggunaan aplikasi game Roblox. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 8643–8650.
- Ramadhan, S. (2024). Peran Media Sosial dalam Kejahatan Siber terhadap Anak. *Jurnal Perlindungan Anak Digital*.
- Ramawan, R. R., & Zaky, M. (2025). Analisis kejahatan siber (cyber child grooming) pada game online Roblox. *Journal of Social Science Research*.
- Wibowo, K. T. (2025). Aspek hukum dalam dunia digital. Sada Kurnia Pustaka.
- Winarni, R. R. (2016). Efektivitas penerapan Undang–Undang ITE dalam tindak pidana cyber crime. *Jurnal Ilmiah Hukum dan Dinamika Masyarakat*, 14(1).