Langkah Bersama Intelekta
Jurnal Inovasi dan Pengabdian Masyarakat (JIPM)
Homepage: https://langkahbersama.id/index.php/jipm
ISSN: 3123 - 3058 (Media Online)
Volume 2, No 3 Mei 2026 (Halaman 376-383)

EDUKASI HUKUM MENGENAI PENCURIAN DATA PRIBADI (PHISHING) PADA PELAJAR SMAN 5 SERANG

Diana Putri[1], Farah Rosa[2], Rafi Fadly[3], Muhamad Abdullah[4], Harry Setiawan[5]
Program Studi Hukum, Fakultas Ilmu Hukum, Universitas Pamulang, Kota Serang, Indonesia[1,2,3,4,5]
Email : putrydiana545@gmail.com[1] , rossacaca6@gmail.com[2], rafifadly68@gmail.com[3], Abdullahmuhamad11636@gmail.com[4] , setiawanharr04@gmail.com[5]

ABSTRAK

Berdasarkan penelitian, abstrak ini membahas edukasi hukum mengenai pencurian data pribadi (phishing) pada pelajar SMAN 5 Serang, penelitian ini dilatarbelakangi oleh maraknya kasus phishing yang menargetkan remaja di Indonesia, termasuk di Banten, seperti insiden penipuan online di Kota Serang pada 2024-2025. Dalam kasus tersebut, pelaku menggunakan teknik phishing untuk mencuri data pribadi siswa melalui aplikasi pesan dan media sosial, dimotivasi oleh keuntungan finansial dan penyalahgunaan identitas. Sumber hukum primer meliputi UU ITE Pasal 32-35 dan putusan pengadilan terkait, sedangkan sumber sekunder berasal dari jurnal serta literatur tentang kejahatan siber. Masalah penelitian mencakup kronologi phishing, dampak pada pelajar, penerapan UU ITE, serta efektivitas edukasi hukum di sekolah. Penelitian menyimpulkan bahwa edukasi hukum preventif diperlukan untuk melindungi pelajar dari phishing, meskipun UU ITE belum sepenuhnya adaptif terhadap evolusi teknologi, sehingga merekomendasikan program literasi digital berbasis sekolah.

Kata kunci: Edukasi Hukum, Pencurian Data Pribadi, Phishing, Pelajar SMAN 5 Serang.

ABSTRACT

Based on the research, this abstract discusses legal education about personal data theft (phishing) in SMAN 5 Serang students, this research is motivated by the rampant phishing cases targeting teenagers in Indonesia, including in Banten, such as the online fraud incident in Serang City in 2024-2025. In those cases, the perpetrators used phishing techniques to steal students' personal data through messaging apps and social media, motivated by financial gain and identity abuse. Primary legal sources include ITE Law Articles 32-35 and related court decisions, while secondary sources come from journals and literature on cybercrime. Research issues include the chronology of phishing, the

Article History
Received: 26 Mei 2026
Reviewed: 28 Mei 2026
Published: 31 Mei 2026

impact on students, the implementation of the ITE Law, and the effectiveness of legal education in schools. The research concludes that preventive legal education is needed to protect students from phishing, even though the ITE Law is not yet fully adaptive to technological evolution, thus recommending school-based digital literacy programs.

Keywords: Legal Education, Personal Data Theft, Phishing, SMAN 5 Serang Students.

PENDAHULUAN

Phishing (pencurian informasi pribadi) tersebar luas yang terjadi di seluruh dunia, termasuk di Indonesia. Para pelaku menggunakan kemajuan teknologi digital yang cepat untuk melakukan berbagai jenis penipuan. Mereka sering menyebarkan tautan palsu atau menyamar sebagai anggota staf perusahaan terkemuka seperti bank, situs e-commerce seperti Shopee, atau organisasi pemerintah lainnya. Mode ini diperkuat oleh narasi yang tampaknya menguntungkan korban misalnya, dengan menawarkan hadiah uang tunai yang mengharuskan mengklik tautan tertentu atau dengan mengarang skenario, seperti berpura-pura menjadi pihak berwenang yang memberi tahu anggota keluarga korban tentang kecelakaan tersebut. Ini memanfaatkan rasa urgensi dan kepanikan korban untuk mengelabui mereka agar mengungkapkan informasi pribadi.

Dampak dari manipulasi psikologis (social engineering) terbukti jauh lebih destruktif dibandingkan dengan penetrasi teknis melalui peretasan sistem yang kompleks. Dalam lanskap kejahatan siber, pelaku memosisikan faktor manusia terutama aspek emosional seperti kepanikan, rasa takut, maupun ekspektasi keuntungan instan sebagai titik lemah utama (the weakest link) dalam sistem keamanan informasi. Ketika korban berada dalam kondisi tekanan psikologis atau desakan urgensi, fungsi kognitif rasional cenderung mengalami penurunan signifikan. Kondisi kelengahan ini dimanfaatkan pelaku untuk mengeksploitasi data sensitif, yang meliputi kredensial otentikasi (seperti username dan PIN perbankan), data finansial (nomor kartu kredit dan kode CVV), hingga instrumen identitas yuridis seperti Nomor Induk Kependudukan (NIK) dan foto KTP. Implikasi dari penguasaan data tersebut tidak hanya berhenti pada kerugian materiil berupa pengurasan saldo rekening secara instan, melainkan juga berlanjut pada tindakan destruktif sekunder, seperti penyalahgunaan identitas untuk pengajuan pinjaman digital ilegal.

Akselerasi inovasi teknologi digital secara parsial turut menggeser karakteristik dan kualitas instrumen penipuan siber. Modus phishing kontemporer telah bertransformasi dari format konvensional yang cenderung rigid dan dipenuhi kesalahan tipografi, menjadi bentuk serangan yang sangat terstruktur dan persuasif.[1] Melalui pemanfaatan komputasi modern, pelaku kini mampu memproduksi narasi yang kredibel, mereplikasi antarmuka situs web resmi (website cloning), serta memalsukan dokumen formal yang identik dengan atribut milik institusi perbankan maupun lembaga negara. Tingginya akurasi visual dan kontekstual pada replika digital ini mengaburkan batas antara informasi valid dan manipulasi, sehingga menurunkan skeptisitas serta daya deteksi masyarakat awam terhadap potensi ancaman siber.

Menyikapi eskalasi ancaman tersebut, formulasi kebijakan edukasi hukum dan literasi digital tidak dapat lagi direduksi sebatas imbauan normatif-prosedural, seperti larangan mengakses tautan asing. Strategi preventif, khususnya bagi kelompok rentan seperti generasi muda dan lansia, harus direorientasikan pada penguatan pemahaman metodologis mengenai

pola-pola manipulasi psikologis. Masyarakat perlu diorientasikan pada kesadaran hukum doktriner bahwa institusi resmi maupun otoritas perbankan tidak memiliki legitimasi operasional untuk meminta data privat atau kode otentikasi (seperti OTP) melalui platform komunikasi informal. Dengan demikian, institusi kebiasaan melakukan verifikasi mandiri secara berlapis (double-check) merupakan bentuk pertahanan mutakhir yang jauh lebih efektif dibandingkan dengan sekadar mengandalkan proteksi teknis pada sistem keamanan digital.

A. IDENTIFIKASI MASALAH

Berdasarkan latar belakang yang telah dipaparkan pada bagian pendahuluan, maka dapat diidentifikasikan beberapa permasalahan utama yang melandasi pentingnya penelitian ini:

1. Pelajar SMAN 5 Serang memiliki tingkat penggunaan gawai yang sangat tinggi baik untuk aktivitas pendidikan maupun hiburan, namun tidak diimbangi dengan literasi hukum siber yang madai. Siswa cenderung tidak menyadari bahaya laten dari penyebaran data pribadi sensitif secara terbuka di ruang digital.
2. Munculnya transformasi serangan phishing yang dinamis dan terstruktur (seperti penggunaan klon situs web, smishing, dan manipulasi dalam transaksi game online) mengeksploitasi aspek psikologis dan kelengahan emosional remaja.
3. Adanya ketidaksesuaian antara aturan normatif (das sollen) dan implementasi riil (das sein) di lapangan. Instrumen hukum seperti UU ITE dan UU PDP dinilai belum sepenuhnya adaptif terhadap evolusi taktik rekayasa sosial (social engineering) serta masih minimnya standardisasi respons cepat penanganan kasus siber di daerah.
4. Banyaknya korban dari kalangan pelajar yang enggan melaporkan atau mendokumentasikan bukti digital kejahatan siber yang dialaminya karena proses birokrasi hukum yang dianggap rumit, berbelit-belit, dan membutuhkan biaya tinggi.
5. Belum adanya model kerja sama yang integratif dan tersinkronisasi dengan baik antara pihak manajemen sekolah, keluarga (orang tua), dan kepolisian dalam upaya penanggulangan hukum secara preventif bagi remaja.

B. TUJUAN KEGIATAN

Secara sistematis, kegiatan PKM ini diselenggarakan dengan tujuan untuk:

1. Membekali pelajar SMAN 5 Serang dengan literasi hukum digital yang mumpuni agar memiliki pemahaman doktriner mengenai pentingnya privasi, hak kepribadian atas data pribadi, serta meminimalkan kebiasaan berbagi informasi pribadi secara berlebihan (oversharing) di ruang publik digital.
2. Melatih kemampuan kognitif dan perilaku protektif praktis pelajar agar tanggap dalam mendeteksi dan menghindari skenario manipulasi psikologis (social engineering), mengidentifikasi situs web tiruan (website cloning), serta mewaspadai penipuan digital yang menyasar ekosistem game online.
3. Memaparkan substansi normatif UU ITE dan UU PDP secara komparatif kepada para siswa, khususnya penekanan terhadap hak perlindungan hukum khusus bagi subjek data anak di bawah usia 18 tahun sebagaimana diatur dalam Pasal 25 UU PDP.
4. Mengikis skeptisitas birokrasi penegakan hukum siber dengan membimbing siswa memahami prosedur teknis pelaporan yang benar, menjaga rantai pembuktian bukti digital forensik (chain of custody), dan mengenali kanal pelaporan resmi seperti patrolisiber.id.
5. Membangun fondasi sinergis terpadu yang menghubungkan institusi sekolah (melalui sosialisasi hukum preventif terstruktur), keluarga (melalui pola asuh digital), dan aparat kepolisian (melalui program penegakan hukum preventif) guna memperkuat ketahanan siber berbasis komunitas.

C. MANFAAT KEGIATAN

Kegiatan PKM siber ini diharapkan dapat memberikan dampak positif dan manfaat multi-dimensional bagi berbagai pihak terkait, antara lain:

1. Bagi Pelajar SMAN 5 Serang
   Siswa memperoleh tameng perlindungan preventif berupa pengetahuan hukum dan teknis yang aplikatif, sehingga terhindar dari potensi kerugian finansial, penyalahgunaan identitas yuridis (seperti pencurian NIK untuk pinjaman online ilegal), serta trauma psikologis akibat kejahatan siber. Pelajar juga memahami langkah-langkah prosedural yang benar untuk mengamankan data dan melaporkan insiden siber kepada pihak berwenang.
2. Bagi Institusi Sekolah (SMAN 5 Serang):
   Membantu sekolah dalam menciptakan lingkungan belajar-mengajar digital yang aman, kondusif, dan bebas dari kejahatan siber. Kegiatan ini juga menjadi masukan berharga bagi perumusan kebijakan kurikulum lokal sekolah mengenai integrasi muatan literasi digital dan hukum siber secara berkelanjutan.
3. Bagi Universitas Pamulang Kampus Serang:
   Merupakan wujud implementasi nyata dari pilar Tri Dharma Perguruan Tinggi, khususnya Pengabdian kepada Masyarakat (PKM), dalam memberikan solusi nyata atas masalah sosiologis-hukum yang berkembang pesat di Kota Serang, Banten.
4. Bagi Aparat Penegak Hukum dan Pemerintah:
   Membantu meringankan beban penegakan hukum represif dengan memperkuat sistem pertahanan preventif masyarakat dari hulu (pelajar), yang pada akhirnya berkontribusi menurunkan angka statistik kejahatan siber nasional secara bertahap.

D. METODE KEGIATAN

Kegiatan Pengabdian kepada Masyarakat (PKM) ini dilaksanakan secara langsung di lingkungan SMAN 5 Serang, Kota Serang, Banten. Dalam pelaksanaannya, tim pengabdi memberikan edukasi hukum yang komprehensif kepada para pelajar mengenai bahaya pencurian data pribadi atau *phishing* yang marak terjadi di ruang digital. Proses kegiatan dilakukan dengan memaparkan substansi hukum terkait, seperti UU ITE dan UU PDP, guna membekali siswa dengan pemahaman mengenai pentingnya menjaga privasi dan hak atas data pribadi mereka. Selain aspek normatif, kegiatan ini juga fokus pada pelatihan keterampilan praktis agar siswa mampu mendeteksi berbagai modus manipulasi psikologis (*social engineering*), seperti pengenalan situs web tiruan atau tawaran hadiah palsu yang sering menyasar remaja. Terakhir, tim memberikan panduan teknis mengenai prosedur pelaporan kejahatan siber melalui kanal resmi seperti patrolisiber.id, sekaligus membangun sinergi antara pihak sekolah, dan juga siswa/siswi untuk memperkuat ketahanan siber di lingkungan pendidikan.

HASIL DAN PEMBAHASAN

1. Tingkat Literasi Hukum Siber Pelajar di SMAN 5 Serang

Literasi hukum siber bagi pelajar di era digital bukan lagi merupakan opsi, melainkan kebutuhan mendasar untuk menjamin keselamatan individu di ruang maya. Berdasarkan observasi dan interaksi langsung dengan siswa di SMAN 5 Serang, ditemukan bahwa terdapat disparitas yang signifikan antara intensitas penguasaan perangkat digital dengan kedalaman pemahaman mengenai risiko serta konsekuensi hukum yang menyertainya. Fenomena ini menciptakan celah (gap) yang lebar antara kemampuan teknis siswa dalam mengoperasikan gawai dengan kemampuan kognitif mereka dalam memproteksi diri dari kejahatan siber.

Mayoritas pelajar di SMAN 5 Serang berada dalam kategori digital natives yang mahir dalam memanfaatkan berbagai platform media sosial, aplikasi pesan instan, dan game online untuk kebutuhan akademis maupun rekreasi. Namun, kemahiran operasional ini tidak berbanding lurus dengan kesadaran hukum. Banyak siswa memandang ruang digital sebagai lingkungan yang "bebas" tanpa batasan, di mana privasi hanyalah sekadar pengaturan yang dapat diabaikan. Literasi hukum siber yang rendah tercermin dari sikap abai terhadap proteksi

data pribadi, seperti membagikan nomor telepon, NIK, atau lokasi real-time kepada pihak yang tidak dikenal di ruang publik digital.

Siswa sering kali gagal memahami bahwa jejak digital mereka memiliki implikasi hukum yang diatur secara ketat dalam UU Informasi dan Transaksi Elektronik (UU ITE) dan UU Pelindungan Data Pribadi (UU PDP). Banyak dari mereka tidak menyadari bahwa pencurian data pribadi (phishing) yang dialami sering kali dimulai dari kelalaian mereka sendiri dalam melakukan otentikasi dua faktor atau mengklik tautan (link) yang tidak kredibel. Secara sosiologis, terdapat anggapan di kalangan pelajar bahwa "data pribadi" adalah informasi yang tidak bernilai finansial, sehingga mereka tidak melihat urgensi untuk melindunginya secara prosedural.

Rendahnya literasi hukum siber di SMAN 5 Serang dipengaruhi oleh beberapa faktor struktural. Pertama, kurikulum formal sekolah saat ini belum secara eksplisit mengintegrasikan muatan hukum siber sebagai bagian dari pendidikan kewarganegaraan atau informatika. Pendidikan digital masih lebih banyak fokus pada teknik penggunaan aplikasi daripada etika dan aspek hukum. Akibatnya, siswa hanya dibekali dengan cara "mengakses", namun tidak dibekali dengan cara "bertahan" atau "melindungi diri" secara hukum. Kedua, pengaruh teman sebaya (peer group) dan tekanan untuk selalu terkoneksi menciptakan budaya di mana privasi dianggap sebagai hambatan dalam bersosialisasi. Adanya normalisasi praktik seperti berbagi kata sandi akun game online atau meminjamkan akun media sosial kepada rekan sejawat menunjukkan bahwa pemahaman mengenai kepemilikan data pribadi dan tanggung jawab hukum atas penggunaan akun tersebut masih sangat minim. Dalam pandangan hukum, setiap tindakan yang dilakukan melalui akun pribadi merupakan tanggung jawab pemilik akun, sebuah realitas yang jarang disadari oleh para pelajar.

Pada akhirnya, literasi hukum siber bagi pelajar bukan sekadar tentang menghafal pasal-pasal dalam perundang-undangan. Ia adalah proses pembangunan karakter dan kesadaran kritis agar pelajar dapat menjadi warga negara digital yang bertanggung jawab. Dengan meningkatkan pemahaman siswa SMAN 5 Serang terhadap hak dan kewajiban mereka di ruang siber, diharapkan lingkungan pendidikan dapat menjadi benteng pertama dalam memutus mata rantai kejahatan siber yang menyasar generasi muda di Kota Serang.

2. Rentan Terhadap Manipulasi Psikologis (Social Engineering)

Dalam lanskap kejahatan siber yang semakin kompleks, fenomena social engineering atau manipulasi psikologis telah menjadi ancaman utama yang mengeksploitasi aspek kemanusiaan sebagai titik terlemah dalam sistem keamanan informasi. Pada dasarnya, social engineering merupakan metode penipuan yang tidak berfokus pada peretasan teknis sistem yang rumit, melainkan pada manipulasi emosional target. Bagi pelajar SMAN 5 Serang, ancaman ini menjadi sangat nyata karena pelaku sering kali menyasar kondisi psikologis remaja yang cenderung mudah panik, merasa takut, atau justru tergiur oleh ekspektasi keuntungan instan. Ketika seseorang berada dalam tekanan emosional atau urgensi yang diciptakan oleh pelaku, fungsi kognitif rasional mereka akan mengalami penurunan yang signifikan, sehingga mereka lebih mudah diarahkan untuk mengungkapkan data sensitif tanpa disadari. Modus operandi yang digunakan oleh para pelaku pun telah mengalami transformasi yang sangat canggih dan terstruktur.

Pelaku tidak lagi sekadar mengirimkan pesan dengan tata bahasa yang berantakan, melainkan kini mampu melakukan replikasi antarmuka situs web resmi (website cloning) dan memalsukan dokumen formal yang sangat menyerupai atribut institusi perbankan maupun lembaga negara. Narasi yang dibangun pun sangat persuasif, misalnya dengan berpura-pura menjadi pihak berwenang yang mengabarkan musibah keluarga, atau menawarkan hadiah uang

tunai melalui tautan tertentu yang mewajibkan korban melakukan verifikasi data. Tingginya akurasi visual dan kontekstual pada replika digital ini sering kali mengaburkan batas antara informasi valid dan manipulasi, yang pada akhirnya menurunkan tingkat skeptisitas serta daya deteksi masyarakat awam, termasuk kalangan pelajar, terhadap ancaman siber yang sedang dihadapi. [2]

Implikasi dari keberhasilan manipulasi psikologis ini sangat destruktif bagi para siswa. Penguasaan terhadap data privat—mulai dari kredensial otentikasi seperti username dan PIN perbankan, hingga identitas yuridis berupa NIK dan foto KTP—tidak hanya berujung pada kerugian materiil seperti pengurasan saldo rekening.[3] Lebih jauh lagi, data yang telah dicuri tersebut dapat disalahgunakan untuk tindakan destruktif sekunder, salah satunya adalah pengajuan pinjaman digital ilegal atas nama korban. Mengingat sifat serangan ini yang menyasar kelengahan emosional, strategi pertahanan yang paling efektif bukanlah sekadar mengandalkan sistem keamanan teknis, melainkan melalui penguatan pemahaman metodologis dan kesadaran hukum bahwa institusi resmi tidak akan pernah meminta data privat melalui platform komunikasi informal. Oleh karena itu, membangun budaya verifikasi mandiri secara berlapis (double-check) menjadi benteng pertahanan mutakhir yang harus dimiliki oleh setiap pelajar agar terhindar dari jeratan manipulasi psikologis di masa depan.

3. Ketidaksesuaian Antara Norma Hukum dan Implementasi

Dalam upaya perlindungan data pribadi, terdapat kesenjangan yang nyata antara norma hukum yang tertulis (*das sollen*) dengan realitas implementasi di lapangan (*das sein*). Meskipun instrumen hukum utama seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Pasal 32-35 dan Undang-Undang Pelindungan Data Pribadi (UU PDP) telah menjadi payung hukum formal, efektivitasnya sering kali terbentur pada kecepatan evolusi taktik kejahatan siber yang bersifat dinamis.[4]

Pelaku kejahatan siber terus melakukan inovasi dalam teknik rekayasa sosial (*social engineering*) yang membuat regulasi yang ada tampak lamban dalam merespons ancaman baru, terutama yang menyasar pengguna muda di tingkat daerah. Ketidaksesuaian ini menciptakan ruang kosong di mana perlindungan bagi subjek data anak di bawah usia 18 tahun, sebagaimana diamanatkan dalam Pasal 25 UU PDP, belum sepenuhnya terinternalisasi dalam praktik penegakan hukum di sekolah maupun instansi terkait. Selain itu, minimnya standardisasi prosedur operasional dalam penanganan cepat kasus siber di daerah sering kali membuat regulasi hanya bersifat normatif-prosedural tanpa dampak preventif yang masif bagi masyarakat awam.[5]

Keadaan ini diperparah dengan belum adanya model kerja sama yang integratif antara pihak sekolah, orang tua, dan aparat kepolisian dalam upaya penanggulangan hukum secara preventif yang mampu menjangkau kebutuhan teknis di lapangan. Akibatnya, hukum sering kali baru menyentuh aspek represif setelah kerugian terjadi, sementara aspek preventif yang seharusnya mendasari kebijakan perlindungan data pribadi belum terimplementasi secara optimal untuk memitigasi risiko sejak dini. Untuk mengatasi celah ini, diperlukan harmonisasi antara substansi undang-undang dengan realitas digital yang dihadapi pelajar, sehingga hukum tidak sekadar menjadi teks mati, melainkan instrumen perlindungan yang adaptif dan responsif terhadap setiap dinamika ancaman siber yang muncul.

4. Kendala Pelaporan dan Birokrasi Penegakan Hukum

Salah satu hambatan fundamental dalam ekosistem penegakan hukum siber di Indonesia adalah rendahnya tingkat pelaporan kasus oleh korban, terutama dari kalangan pelajar. Fenomena ini berakar dari persepsi publik yang mendalam bahwa prosedur birokrasi penegakan hukum siber dianggap sebagai proses yang sangat rumit, berbelit-belit, dan membutuhkan biaya yang tidak sedikit. Bagi pelajar di SMAN 5 Serang, ketika menghadapi insiden seperti *phishing* atau pencurian identitas, ketidaktahuan akan kanal pelaporan resmi sering kali membuat mereka memilih untuk diam daripada menempuh jalur hukum yang formal.

Ketidakberanian untuk melapor ini diperburuk oleh minimnya pemahaman mengenai pentingnya menjaga rantai pembuktian atau *chain of custody* atas bukti digital yang mereka miliki.[6] Padahal, bukti digital yang valid dan terjaga keutuhannya merupakan instrumen krusial dalam proses penyidikan kejahatan siber. Selain itu, terdapat skeptisisme yang luas di kalangan remaja mengenai efektivitas respons aparat penegak hukum terhadap pengaduan yang masuk, yang dipicu oleh pengalaman atau narasi negatif mengenai panjangnya durasi penanganan kasus di tingkat daerah.

Hal ini menciptakan tantangan besar dalam upaya penegakan hukum yang bersifat represif, karena laporan dari masyarakat merupakan pintu masuk utama bagi kepolisian untuk melakukan tindakan hukum. Oleh karena itu, perlu adanya upaya edukasi yang intensif untuk mengikis skeptisisme birokrasi tersebut dengan cara mengenalkan kanal pelaporan yang kredibel dan mudah diakses, seperti portal resmi patrolisiber.id. Melalui sosialisasi yang berkelanjutan, pelajar diharapkan tidak hanya memahami mekanisme teknis dalam menjaga bukti digital, tetapi juga menyadari bahwa setiap laporan yang mereka berikan merupakan langkah vital dalam memperkuat sistem keamanan siber nasional dan mencegah jatuhnya korban baru di kemudian hari.

5. Kebutuhan Sinergi Antar-Stakeholder

Penanggulangan kejahatan siber yang menyasar generasi muda, khususnya pelajar di SMAN 5 Serang, tidak dapat diselesaikan secara parsial oleh satu pihak saja. Kompleksitas ancaman *phishing* dan rekayasa sosial menuntut adanya model kerja sama yang integratif dan tersinkronisasi dengan baik antara manajemen sekolah, keluarga (orang tua), dan aparat kepolisian. Institusi sekolah memegang peranan krusial sebagai pusat edukasi formal dengan menyelenggarakan sosialisasi hukum preventif yang terstruktur dan berkelanjutan untuk meningkatkan literasi digital siswa. Namun, efektivitas pendidikan di sekolah akan kehilangan momentumnya jika tidak didukung oleh pola asuh digital yang konsisten di lingkungan keluarga.

Orang tua harus berperan sebagai pendamping yang mampu memantau aktivitas digital anak dan memberikan edukasi dasar mengenai privasi sejak dini di rumah, sehingga tercipta pengawasan yang berlapis. Di sisi lain, keterlibatan aparat kepolisian melalui program penegakan hukum preventif sangat diperlukan untuk memberikan pemahaman mengenai konsekuensi yuridis, prosedur pelaporan yang tepat, serta memberikan rasa aman kepada pelajar sebagai subjek hukum yang rentan.

Sinergi antara ketiga pihak ini menciptakan ekosistem perlindungan yang holistik, di mana sekolah menyediakan kurikulum hukum, orang tua memberikan pengawasan keseharian, dan kepolisian menyediakan kerangka penegakan hukum yang responsif. Dengan membangun fondasi sinergis terpadu ini, komunitas sekolah dapat bertransformasi menjadi komunitas yang memiliki ketahanan siber (*cyber resilience*) yang kuat. Pendekatan kolaboratif ini bukan hanya berfungsi sebagai benteng pertahanan bagi pelajar dari upaya eksploitasi data pribadi, tetapi

juga berkontribusi secara nyata dalam menurunkan angka statistik kejahatan siber nasional dari sisi hulu, yakni kelompok pelajar yang saat ini menjadi target utama serangan digital. Oleh karena itu, sinergi antar-*stakeholder* ini harus diinstitusionalisasikan dalam bentuk program kerja sama yang jelas dan berkelanjutan, bukan sekadar kegiatan insidental, guna memastikan setiap pihak memahami peran dan tanggung jawabnya dalam menciptakan ruang digital yang lebih aman bagi generasi muda di masa depan.

KESIMPULAN DAN SARAN

Kesimpulan

Kegiatan pengabdian masyarakat ini menyimpulkan bahwa pelajar SMAN 5 Serang memiliki ketergantungan yang tinggi terhadap perangkat digital, namun hal ini tidak diimbangi dengan tingkat literasi hukum siber yang memadai. Kerentanan utama yang ditemukan adalah rendahnya kewaspadaan terhadap modus *social engineering* yang semakin canggih, seperti penggunaan klon situs web dan manipulasi psikologis, yang sering kali mengeksploitasi kelengahan emosional remaja. Selain itu, terdapat kesenjangan signifikan antara norma hukum (UU ITE dan UU PDP) dengan implementasi di lapangan, yang diperburuk oleh persepsi pelajar mengenai rumitnya birokrasi pelaporan kejahatan siber. Secara substansial, upaya perlindungan pelajar dari kejahatan siber tidak dapat hanya mengandalkan aspek teknis, melainkan harus didukung oleh integrasi literasi hukum siber dalam lingkungan sekolah dan keluarga.

Saran

- Bagi Pihak Sekolah, disarankan untuk mengintegrasikan kurikulum literasi digital dan hukum siber ke dalam kegiatan ekstrakurikuler atau muatan lokal guna membangun budaya sadar hukum sejak dini.
- Bagi Siswa, diharapkan untuk selalu menerapkan verifikasi mandiri (double-check) sebelum membagikan data pribadi di platform digital dan memahami prosedur resmi pelaporan melalui kanal seperti patrolisiber.id.
- Bagi Aparat Penegak Hukum, disarankan untuk terus menyosialisasikan kemudahan prosedur pelaporan kejahatan siber agar skeptisisme masyarakat terhadap birokrasi hukum dapat terkikis.

DAFTAR PUSTAKA

Hidayat, R., & Santoso, B. (2025). "Kesenjangan Antara Regulasi dan Praktik Penegakan Hukum Siber di Indonesia". *Jurnal Kebijakan Publik dan Hukum*, 14(1), 55-72.

Januponsa Dio Firizqi, Valentinus Putra Setiawan, and Universitas Pradita, “Analisis Serangan Social Engineering Melalui Pretexting , Impersonating , Dan Phishing Pada Pemain Game Mobile Online Analysis of Social Engineering Attacks Through Pretexting , Impersonating , and Phishing on Online Mobile Game Players,” *Jurnal Pendidikan Dan Teknologi Indonesia (JPTI)* 5, no. 7 (2025): 1981–92.

Kurniawan, E. (2024). "Problematika *Chain of Custody* dalam Pembuktian Bukti Digital pada Kasus *Phishing*". *Jurnal Penegakan Hukum Siber*, 7(3), 45-60.

N. A., & Salsabila, H. (2025). "Analisis Kerentanan *Social Engineering* pada Pengguna Media Sosial di Kalangan Remaja". *Jurnal Siber dan Hukum Indonesia*, 12(2), 145-160.

Prasetyo, T. (2024). *Perlindungan Data Pribadi: Teori dan Praktik dalam Sistem Hukum Indonesia*. Jakarta: Rineka Cipta.

Wijaya, K. (2024). "Perlindungan Data Pribadi dan Tantangan Literasi Digital dalam Menghadapi Phishing Kontemporer". *Jurnal Komunikasi dan Informatika*, 8(1), 22-38.