



Edukasi Keamanan Siber Pada Penipuan Online Penyebaran Link Palsu

Sherny Denisa Sari¹, Cindy Eka Amalia², Nurhalisa³, Risna⁴, Mela Meliani⁵,
Anggie Selviana⁶, Salwa Salsabila Aulia Ridwan⁷, Sunariyo⁸

Fakultas Hukum, Universitas Muhammadiyah Kalimantan Timur, Indonesia¹⁻⁸

Email Korespondensi: 2311102432133@umkt.ac.id, 2311102432041@umkt.ac.id,
2311102432134@umkt.ac.id, 2311102432012@umkt.ac.id, 2311102432117@umkt.ac.id,
2311102432102@umkt.ac.id, 2311102432107@umkt.ac.id, sun487@umkt.ac.id

Article received: 15 September 2025, Review process: 25 September 2025

Article Accepted: 10 Oktober 2025, Article published: 11 Desember 2025

ABSTRACT

This community engagement activity was carried out as an implementation of the Tri Dharma of Higher Education, focusing on strengthening school communities' awareness of cyber security threats, particularly online fraud through the circulation of fake links (phishing). The objective of this program was to enhance students' digital literacy and deepen their understanding of legal aspects related to personal data misuse and risky online behavior. The methods involved material presentation, interactive discussions, case studies, and prevention simulations delivered to 30 students of SMK Istiqomah Muhammadiyah 4 Samarinda. The results indicate a significant improvement in participants' ability to identify fake links, understand digital fraud schemes, and apply preventive measures to protect personal data. The implications highlight that cyber security education is essential for fostering a culture of digital literacy and cyber-law awareness within educational environments.

Keywords: Cyber Security, Online Fraud, Fake Links, Digital Literacy, Cyber Law

ABSTRAK

Kegiatan pengabdian ini dilaksanakan sebagai bentuk implementasi Tri Dharma Perguruan Tinggi yang berfokus pada peningkatan kesadaran masyarakat sekolah terhadap ancaman keamanan siber, khususnya penipuan online melalui penyebaran link palsu (phishing). Tujuan kegiatan adalah memperkuat literasi digital siswa serta memberikan pemahaman mengenai aspek hukum terkait penyalahgunaan data pribadi dan aktivitas daring berisiko. Metode pelaksanaan mencakup pemaparan materi, diskusi interaktif, studi kasus, dan simulasi pencegahan yang diterapkan kepada 30 siswa SMK Istiqomah Muhammadiyah 4 Samarinda. Hasil kegiatan menunjukkan peningkatan signifikan pada kemampuan peserta dalam mengenali ciri-ciri link palsu, memahami modus penipuan digital, serta menerapkan langkah pencegahan untuk menjaga keamanan data pribadi. Implikasi kegiatan ini menegaskan bahwa edukasi keamanan siber merupakan langkah strategis dalam membangun budaya literasi digital dan kesadaran hukum siber di lingkungan pendidikan.

Kata Kunci: Keamanan Siber, Penipuan Online, Link Palsu, Literasi Digital, Hukum Siber

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital saat ini telah membawa dampak besar bagi dunia pendidikan. Hampir seluruh aktivitas belajar dan interaksi siswa kini dilakukan secara daring (R. M. Santoso, 2022), baik melalui media sosial, platform pembelajaran, maupun layanan internet lainnya. Internet memberikan kemudahan dalam mencari informasi dan memperluas wawasan, namun disisi lain juga membuka peluang terjadinya berbagai ancaman kejahatan siber (cybercrime). Salah satu ancaman yang paling sering dialami oleh kalangan pelajar adalah penipuan online melalui penyebaran link palsu atau yang dikenal istilah phishing.

Penipuan online dengan modus penyebaran link palsu dilakukan dengan cara menyebarkan tautan melalui pesan singkat, media sosial, maupun email yang tampak seperti berasal dari sumber resmi seperti sekolah atau lembaga pendidikan tertentu. Banyak siswa yang tidak menyadari bahaya tautan tersebut, sehingga secara tidak sengaja memberikan informasi pribadi seperti akun media sosial, alamat email, hingga kata sandi. Data tersebut kemudian dapat digunakan oleh pelaku kejahatan untuk melakukan penipuan, pencurian akun, bahkan penyebaran informasi palsu atas nama korban.

Fenomena ini menunjukkan bahwa siswa masih memiliki tingkat kewaspadaan yang rendah terhadap keamanan digital. Berdasarkan data dari badan siber dan sandi negara (BSSN) tahun 2024, tercatat lebih dari 370 juta serangan siber di Indonesia, dimana sebagian besar berasal dari modus phishing dan penipuan daring. Kondisi ini memperlihatkan bahwa literasi digital di kalangan pelajar perlu terus ditingkatkan. Banyak siswa yang masih belum memahami cara mengenali link palsu, bagaimana melindungi data pribadi, serta apa konsekuensi hukumnya jika terlibat dalam penyebaran informasi berbahaya tersebut.

Oleh karena itu, diperlukan kegiatan edukasi keamanan siber kepada siswa untuk meningkatkan kesadaran dan pemahaman mereka mengenai pentingnya menjaga keamanan data pribadi di dunia maya. Edukasi ini diharapkan dapat membekali siswa dengan pengetahuan dasar tentang bagaimana cara mengenali tautan palsu, memahami dampak hukum dari kejahatan siber, serta membentuk kebiasaan positif dalam menggunakan internet secara aman dan bertanggung jawab.

Kegiatan pengabdian ini dilaksanakan dalam rangkapenerapan mata kuliah hukum siber, yang tidak hanya menegakan aspek teori, tetapi juga praktik penerapan hukum dalam konteks sosial dan pendidikan. Melalui kegiatan ini, mahasiswa berperan sebagai agen perubahan yang memberikan pemahaman hukum dan literasi digital kepada siswa, edukasi semacam ini diharapkan dapat membantu siswa lebih waspada terhadap kejahatan siber dan mampu bertindak dengan bijak saat beraktivitas di dunia digital.

Secara yuridis, penyebaran link palsu dan pengabdian data pribadi tanpa izin merupakan pelanggaran hukum sebagaimana diatur dalam undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) sebagaimana telah diubah dengan UU Nomor 11 Tahun 2016. Pasal 30 dan 32 UU ITE menegaskan bahwa setiap orang dengan sengaja tanpa hak mengakses sistem

elektronik orang lain atau memindahkan data elektronik secara ilegal dapat dikenakan sanksi pidana. Selain itu, undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi (UU PDP) juga mengatur perlindungan terhadap informasi pribadi yang sering menjadi sasaran utama dalam kasus kejahatan digital.

Dengan memahami dasar hukum tersebut, siswa diharapkan menyadari bahwa keamanan siber bukan hanya masalah teknis, tetapi juga memiliki aspek hukum yang penting. Penyebaran link palsu, meskipun tampak sederhana (K. T. Nugroho, 2023), dapat menimbulkan kerugian besar baik bagi korban maupun pelaku yang dapat dikenai sanksi pidana. Karena itu, edukasi ini menjadi langkah preventif untuk mencegah terjadinya kejahatan siber di lingkungan sekolah.

Kegiatan ini diharapkan memberikan manfaat teoritis dan praktis. Secara teoritis, kegiatan ini memperkuat penerapan konsep hukum siber dalam bidang pendidikan dan perlindungan data pribadi. Selain itu, bagi mahasiswa, kegiatan ini menjadi pengalaman nyata dalam menerapkan ilmu hukum siber secara langsung dilapangan melalui kegiatan edukasi dan pengabdian kepada sekolah.

Dengan dilaksanakannya kegiatan "Edukasi Keamanan Siber pada Penipuan Online Penyebaran Link Palsu", diharapkan siswa dapat menjadi generasi yang cerdas digital, paham hukum, dan mampu menjaga keamanan data pribadi di era teknologi yang terus berkembang. Kegiatan ini sekaligus menjadi wujud nyata penerapan Tri Dharma Perguruan Tinggi, khususnya dalam bidang pengabdian kepada masyarakat melalui pendekatan edukatif di lingkungan sekolah.

METODE

Metode pelaksanaan kegiatan dirancang melalui empat tahapan terpadu yang meliputi identifikasi awal pemahaman peserta mengenai keamanan siber melalui pre-test, penyajian materi edukatif tentang konsep phishing dan perlindungan data pribadi melalui pendekatan ceramah dan diskusi, pelatihan aplikatif melalui simulasi analisis link palsu dan perbandingan situs resmi dengan situs tiruan, serta evaluasi akhir melalui post-test untuk mengukur peningkatan pengetahuan dan perubahan perilaku digital peserta; keseluruhan rangkaian ini digunakan untuk memastikan bahwa kegiatan tidak hanya bersifat informatif, tetapi juga mampu menumbuhkan keterampilan praktis dan kesadaran hukum siber secara komprehensif.

HASIL DAN PEMBAHASAN

Peningkatan Kesadaran Keamanan Siber

Hasil pengukuran pre-test dan post-test menunjukkan peningkatan pemahaman peserta sebesar 65% dalam mengenali ciri-ciri penipuan online. Sebelum edukasi, sebagian besar peserta belum memahami bahwa link palsu dapat disamarkan menggunakan domain mirip, misalnya bankindo.co menggantikan bankindonesia.go.id. Setelah edukasi, peserta mampu mengidentifikasi perbedaan kecil pada struktur domain, serta memahami pentingnya sertifikat keamanan (HTTPS).

Strategi Pencegahan Penipuan Link Palsu

Materi edukasi menekankan pentingnya beberapa langkah pencegahan utama:

1. Memeriksa alamat URL dan tanda gembok pada browser sebelum membuka tautan
2. Tidak mengklik tautan dari sumber tidak dikenal
3. Menggunakan password manager dan autentikasi dua langkah
4. Menghindari memberikan data pribadi melalui formulir online yang mencurigakan.

Peserta juga diperkenalkan dengan peraturan hukum terkait keamanan data seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 jo. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) yang memberikan dasar hukum terhadap perlindungan privasi dan penegakan hukum terhadap pelaku kejahatan siber.

Dampak Kegiatan terhadap Literasi Digital

Dari hasil evaluasi, kegiatan ini berhasil menumbuhkan sikap waspada dan tanggung jawab digital di kalangan peserta. Sebagian peserta mulai menerapkan pengamanan tambahan pada akun media sosial dan email pribadi. Selain itu, mahasiswa peserta kegiatan berkomitmen untuk menyebarluaskan pengetahuan ini melalui program cyber awareness di lingkungan kampus. Kegiatan ini juga menumbuhkan kesadaran hukum digital, di mana masyarakat memahami bahwa penyebaran link palsu bukan sekadar pelanggaran etika tetapi merupakan tindak pidana siber sebagaimana diatur dalam Pasal 28 ayat (1) UU ITE. Oleh karena itu, kegiatan edukasi ini tidak hanya meningkatkan pengetahuan teknis tetapi juga kesadaran hukum masyarakat.

SIMPULAN

Kegiatan pengabdian kepada masyarakat yang mengangkat tema “Edukasi Keamanan Siber pada Penipuan Online Penyebaran Link Palsu” telah dilaksanakan pada tanggal 13 Oktober 2025, bertempat pada SMK Istiqomah Muhammadiyah 4 Samarinda di Jl.A Wahab Syahraie, RT.25, Air Hitam kec.Samarinda ulu. Kegiatan ini merupakan bagian dari program pengabdian Universitas Muhammadiyah Kalimantan Timur yang mana bertujuan untuk memberikan dampak positif terhadap peningkatan pemahaman dan kesadaran masyarakat mengenai ancaman penipuan berbasis tautan digital. Melalui metode edukatif dan simulatif, peserta memperoleh kemampuan untuk mengenali link palsu, menerapkan langkah pencegahan, serta memahami aspek hukum dari kejahatan siber. Kegiatan ini membuktikan bahwa literasi digital merupakan kunci utama dalam menciptakan ruang siber yang aman dan bertanggung jawab. Diharapkan hasil kegiatan ini dapat menjadi model edukasi berkelanjutan yang diterapkan di berbagai lingkungan sosial dan pendidikan, guna menekan angka kejahatan siber di Indonesia.

UCAPAN TERIMA KASIH

Kami menyampaikan apresiasi dan terima kasih yang sebesar-besarnya kepada Program Studi S1 Hukum Universitas Muhammadiyah Kalimantan Timur atas dukungan pendanaan dan fasilitas yang telah diberikan dalam pelaksanaan kegiatan Pengabdian ini. Serta kami ucapkan terima kasih juga kepada SMK Itiqomah Muhammadiyah 4 Samarinda beserta seluruh pihak yang telah mendukung kegiatan ini sehingga dapat terlaksana dengan baik. Serta penghargaan kepada siswa/i SMK 4 Itiqomah Muhammadiyah 4 Samarinda yang berhasil melibatkan 30 siswa/i sebagai peserta aktif yang menunjukkan antusiasme tinggi dalam mengikuti sosialisasi Edukasi Keamanan Siber Pada Penipuan Online Penyebaran Link Palsu.

DAFTAR PUSTAKA

- Iswanto, A. (2024). *Cyber Hygiene: Membangun Kesadaran Digital di Era Disrupsi*. Yogyakarta: Deepublish.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Laporan Tahunan Keamanan Siber Nasional*. Jakarta: Kominfo.
- Prasetyo, R., & Hidayat, N. (2023). Pendekatan Preventif Terhadap Kejahatan Siber di Kalangan Mahasiswa. *Jurnal Hukum dan Teknologi*, 2(3), 215–229.
- Raharjo, D. (2023). Analisis Modus Penipuan Online di Indonesia dan Strategi Pencegahannya. *Jurnal Siber dan Informasi*, 5(2), 101–115.
- Sari, R. A., & Putra, M. D. (2022). Peningkatan Literasi Digital dalam Pencegahan Kejahatan Siber. *Jurnal Edukasi Teknologi*, 3(1), 44–53.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 19 Tahun 2016.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.