

## PELATIHAN PERLINDUNGAN DATA DAN KEAMANAN SIBER UNTUK MASYARAKAT DI LKP MUTIARA INFORMATIKA KABUPATEN ASAHAN

**Irianto<sup>1\*</sup>, Andri Nata<sup>2</sup>, Sumantri<sup>3</sup>**

<sup>1,2</sup>Sistem Informasi, Universitas Royal

<sup>3</sup>Hukum, Universitas Royal

*email: irianto2121212@gmail.com*

**Abstract:** The rapid development of digital technology brings various benefits as well as challenges, one of which is the increasing risk of cyber threats and personal data breaches. The digital community, particularly participants at LKP Mutiara Informatika in Asahan Regency, requires a fundamental understanding and skills in protecting personal data and recognizing cyber threats. This community service program aims to provide educational and practical training on personal data protection and cybersecurity. The implementation methods include material delivery, interactive discussions, and practical simulations using real case studies. This program enhanced participants' understanding of digital privacy, online fraud, and the use of basic security tools. Participants were also able to identify preventive measures to protect their digital accounts. Through this training, the community is better prepared to face the challenges of the technological era and to serve as agents of cybersecurity literacy, while also emphasizing the importance of synergy between education and technology in building safe and responsible digital awareness.

**Keywords:** personal data; cybersecurity; digital community

**Abstrak:** Perkembangan teknologi digital yang pesat membawa berbagai manfaat sekaligus tantangan, salah satunya adalah meningkatnya risiko terhadap keamanan siber dan kebocoran data pribadi. Masyarakat digital, khususnya peserta di LKP Mutiara Informatika Kabupaten Asahan, membutuhkan pemahaman dan keterampilan dasar dalam melindungi data pribadi serta mengenali ancaman siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk memberikan pelatihan yang bersifat edukatif dan aplikatif mengenai perlindungan data pribadi dan keamanan siber. Metode pelaksanaan meliputi penyampaian materi, diskusi interaktif, dan simulasi praktik menggunakan studi kasus nyata. Kegiatan ini meningkatkan pemahaman peserta tentang privasi digital, penipuan online, serta penggunaan perangkat pengaman dasar. Peserta juga mampu mengenali langkah pencegahan untuk melindungi akun digital. Dengan pelatihan ini, masyarakat lebih siap menghadapi tantangan era teknologi dan berperan sebagai agen literasi keamanan siber, sekaligus menegaskan pentingnya sinergi edukasi dan teknologi dalam membangun kesadaran digital yang aman.

**Kata kunci:** data pribadi; keamanan siber; masyarakat digital

## PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa masyarakat ke dalam era digital, di mana hampir seluruh aktivitas, baik pribadi maupun profesional, dilakukan secara daring (*online*). Mulai dari transaksi keuangan, komunikasi, layanan publik, hingga pendidikan dan pekerjaan kini bergantung pada infrastruktur digital. Namun, seiring dengan kemudahan tersebut, muncul pula ancaman serius terhadap keamanan data pribadi yang seringkali tidak disadari oleh pengguna (Ghalib et al., 2024). Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami peningkatan signifikan dalam jumlah insiden siber setiap tahunnya. Pada tahun 2023 saja, tercatat lebih dari 300 juta upaya serangan siber, termasuk kebocoran data pribadi, penipuan daring, dan peretasan akun. Hal ini menunjukkan bahwa kesadaran masyarakat Indonesia terhadap pentingnya keamanan siber dan perlindungan data pribadi masih sangat rendah. (Judijanto & Nugroho, 2025)

Maraknya kasus pencurian data pribadi, seperti yang terjadi dalam kebocoran data pelanggan e-commerce, aplikasi kesehatan, hingga data pemerintahan, menjadi alarm penting bagi semua kalangan. Di sisi lain, banyak masyarakat, khususnya di tingkat pengguna pemula atau lembaga pelatihan seperti LKP (Lembaga Kursus dan Pelatihan), belum memiliki bekal pengetahuan dan keterampilan yang memadai dalam mengelola keamanan digital mereka.

Beberapa upaya telah dilakukan oleh pemerintah dan organisasi non-profit untuk mendukung masyarakat tentang literasi digital dan keamanan siber. Misalnya, Kominfo telah meluncurkan program *Gerakan Nasional*

*Literasi Digital* yang salah satu fokusnya adalah keamanan digital. Namun, cakupan program-program ini belum sepenuhnya menyentuh lapisan masyarakat lokal yang menjadi peserta aktif pelatihan di lembaga-lembaga pendidikan nonformal seperti LKP Mutiara Informatika. (Sulubara, 2024)

Atas dasar kondisi tersebut, kegiatan pengabdian masyarakat ini dirancang sebagai respons terhadap kebutuhan peningkatan kesadaran dan keterampilan masyarakat digital dalam menjaga keamanan data pribadi. LKP Mutiara Informatika sebagai mitra pelaksana dipilih karena memiliki peserta didik yang berasal dari berbagai kalangan usia dan latar belakang yang aktif menggunakan teknologi dalam kehidupan sehari-hari namun belum memiliki pemahaman cukup mengenai keamanan siber. (Tommy & Nasution, 2025)

Melalui pelatihan ini, diharapkan peserta memiliki kemampuan dasar dalam mengenali potensi risiko digital, mengetahui hak-hak atas data pribadinya, serta menerapkan langkah-langkah preventif untuk menjaga keamanan data dalam aktivitas digital mereka.

## METODE

Metode pelaksanaan kegiatan pengabdian ini dirancang secara sistematis dan partisipatif agar mampu memberikan pemahaman serta keterampilan praktis kepada peserta dalam melindungi data pribadi dan meningkatkan keamanan siber. (Na, 2025) Kegiatan dilaksanakan dalam beberapa tahapan, sebagai berikut:

### Identifikasi Permasalahan

Tahap awal dilakukan dengan observasi dan wawancara terhadap pengelola serta peserta pelatihan di LKP

Mutiara Informatika untuk mengetahui tingkat pemahaman mereka terhadap pentingnya perlindungan data pribadi dan keamanan siber. Ditemukan bahwa mayoritas peserta belum memahami risiko penggunaan internet tanpa perlindungan data, serta minimnya literasi keamanan digital.

### Perencanaan Program Pelatihan

Tim pengabdian merancang modul pelatihan yang mencakup (1) Pengertian data pribadi dan bahayanya jika disalahgunakan. (2) Ancaman siber yang sering terjadi (phishing, malware, pencurian identitas). (3) Langkah praktis menjaga keamanan data pribadi (password management, enkripsi, VPN). (4) Praktik langsung penggunaan tools keamanan dasar. Selain itu, disiapkan juga media pembelajaran seperti presentasi, video tutorial, dan lembar kerja latihan.

### Pelaksanaan Pelatihan

Pelatihan dilaksanakan dalam bentuk **Sesi teoritis**: Pemaparan materi oleh narasumber menggunakan metode ceramah interaktif dan diskusi. **Sesi praktik**: Peserta melakukan simulasi perlindungan data di perangkat mereka, seperti mengaktifkan autentikasi dua faktor, menggunakan antivirus, serta mengidentifikasi situs palsu. **Studi kasus**: Analisis kasus nyata pelanggaran data pribadi dan upaya pencegahannya. Kegiatan ini dilaksanakan pada 24 Juni 2025 secara tatap muka di ruang teori LKP Mutiara Informatika Kabupaten Asahan.

### Evaluasi dan Tindak Lanjut

Hasil observasi selama kegiatan juga memperlihatkan keterlibatan yang tinggi, di mana **90% peserta** aktif bertanya, berdiskusi, dan mengikuti praktik secara langsung, sementara hanya **10%**

yang terpantau kurang aktif. Selain itu, melalui sesi refleksi kelompok, seluruh peserta (**100%**) menyatakan materi mudah dipahami dan menambah wawasan baru, serta **90%** menilai materi sangat relevan dengan kebutuhan sehari-hari.

## PEMBAHASAN

Pengabdian kepada Masyarakat (PkM) ini bertempat di LKP Mutiara Informatika Kabupaten Asahan yang dilaksanakan 25 Juni 2025 bertujuan untuk membekali masyarakat dengan pengetahuan dan keterampilan esensial dalam menjaga keamanan data pribadi dan aktivitas daring mereka. Dalam era masyarakat digital saat ini, di mana sebagian besar interaksi sosial, ekonomi, dan informasi beralih ke ranah siber, pemahaman akan perlindungan data pribadi (PDP) dan keamanan siber bukan lagi pilihan, melainkan sebuah kebutuhan mendesak.

Pelatihan ini diselenggarakan di LKP Mutiara Informatika, sebuah lembaga yang memiliki akses langsung ke komunitas yang ingin meningkatkan literasi digitalnya. Pemilihan lokasi ini strategis karena LKP sering menjadi pusat pembelajaran dan pengembangan keterampilan di tingkat lokal, sehingga memudahkan partisipasi masyarakat.



Gambar 1. Pemaparan Materi

Target peserta terdiri dari berbagai latar belakang, mulai dari pelajar, pelaku UMKM, hingga ibu rumah tangga yang aktif menggunakan platform digital.



Gambar 2. Peserta Kegiatan PKM

Materi pelatihan dirancang komprehensif, mencakup aspek-aspek krusial seperti:

**Pengenalan Konsep Data Pribadi dan Privasi:** Peserta diperkenalkan pada definisi data pribadi, jenis-jenisnya, serta pentingnya privasi dalam kehidupan daring. Diskusi meliputi data apa saja yang dianggap sensitif dan mengapa perlu dilindungi.

**Ancaman Keamanan Siber:** Modul ini menjelaskan berbagai jenis ancaman siber yang umum terjadi, seperti *phishing*, *malware*, *ransomware*, penipuan *online*, dan *doxing*. Pemahaman terhadap modus operandi para pelaku kejahatan siber sangat ditekankan agar peserta dapat mengenali tanda-tanda bahaya.

**Praktik Perlindungan Data Pribadi:** Sesi ini berfokus pada langkah-langkah praktis yang dapat dilakukan individu, seperti membuat kata sandi yang kuat dan unik, mengaktifkan autentikasi dua faktor (2FA), memahami pengaturan privasi di media sosial, dan berhati-hati dalam berbagi informasi pribadi di internet.

### **Keamanan Transaksi Online:**

Mengingat maraknya aktivitas belanja *online* dan layanan perbankan digital, materi ini membimbing peserta untuk melakukan transaksi secara aman, mengenali situs web atau aplikasi palsu, serta memahami risiko penggunaan Wi-Fi publik untuk transaksi sensitif.

**Peran Undang-Undang Perlindungan Data Pribadi:** Peserta diberikan pemahaman dasar mengenai hak-hak mereka sebagai pemilik data dan kewajiban penyedia layanan dalam melindungi data. Ini termasuk informasi tentang UU PDP di Indonesia dan bagaimana melaporkan pelanggaran.

Metode pelatihan yang digunakan bersifat interaktif, memadukan presentasi, diskusi kelompok, studi kasus nyata, dan simulasi praktis. Pendekatan ini memungkinkan peserta untuk tidak hanya menerima informasi, tetapi juga menginternalisasi dan mempraktikkan pengetahuan yang diperoleh. Misalnya, peserta diajak untuk secara langsung memeriksa pengaturan privasi akun media sosial mereka atau mengidentifikasi contoh email *phishing* (Adma et al., 2023). Respons dari masyarakat sangat positif. Banyak peserta yang mengungkapkan bahwa pelatihan ini membuka mata mereka terhadap risiko yang selama ini kurang disadari. Mereka merasa lebih berdaya dan percaya diri dalam mengelola jejak digital mereka. Dampak yang diharapkan dari PkM ini adalah peningkatan kesadaran dan kapasitas masyarakat dalam menghadapi tantangan keamanan siber, sehingga dapat mengurangi potensi menjadi korban kejahatan *online*. Lingkungan digital yang lebih aman dan terinformasi akan berkontribusi pada terciptanya masyarakat digital yang lebih cerdas dan resilien.

Evaluasi dilakukan melalui **Kuesioner Pre-Test dan Post-Test** dengan tujuan untuk mengukur peningkatan pengetahuan peserta sebelum dan sesudah pelatihan.

Tabel 1. Pre-Test dan Post-Test

Aspek Pengetahuan	Rata-rata Nilai Pre-Test	Rata-rata Nilai Post-Test	Peningkatan (%)
Privasi Digital	52	85	33%
Modus Penipuan Online	48	82	34%
Penggunaan Antivirus & Password Manager	45	80	35%
Rata-rata Keseluruhan	48,3	82,3	+34%

**Interpretasi:** Terdapat peningkatan rata-rata **34%** pemahaman peserta setelah mengikuti pelatihan.

**Observasi Keterlibatan Peserta**  
 Aspek yang diamati: keaktifan bertanya, berdiskusi, dan mengikuti praktik.

Tabel 2. Observasi Keterlibatan Peserta

Kategori Keterlibatan	Jumlah Peserta	Persentase
Sangat Aktif	4	40%
Aktif	5	50%
Kurang Aktif	1	10%

**Interpretasi:** Sebanyak **90%** peserta terlibat aktif dalam kegiatan.

**Refleksi Kelompok** Melalui sesi diskusi dan refleksi kelompok, peserta

memberikan penilaian terhadap manfaat pelatihan:

Tabel 3. Refleksi Kelompok

Aspek	Setuju (%)	Tidak Setuju (%)
Materi mudah dipahami	100%	0%
Menambah wawasan baru	100%	0%
Relevan dengan kebutuhan sehari-hari	90%	10%
Termotivasi menerapkan keamanan digital	100%	0%

**Interpretasi:** Mayoritas peserta menilai pelatihan bermanfaat, relevan, dan mudah dipahami.

Pelatihan berhasil meningkatkan pengetahuan peserta sebesar 34%, dengan 90% peserta aktif terlibat, dan hampir seluruh peserta merasa pelatihan bermanfaat. Keberlanjutan dilakukan melalui grup komunikasi daring sebagai media konsultasi dan pembinaan.

## SIMPULAN

Kegiatan pelatihan perlindungan data pribadi dan keamanan siber yang dilaksanakan di LKP Mutiara Informatika telah berhasil meningkatkan pemahaman dan kesadaran peserta terhadap pentingnya menjaga data pribadi di era digital. Peserta pelatihan menunjukkan antusiasme tinggi dalam mengikuti materi yang disampaikan, mulai dari pengenalan jenis-jenis ancaman siber, cara mengamankan perangkat digital, hingga langkah-langkah praktis dalam menjaga

kerahasiaan informasi pribadi di dunia maya. Pelatihan ini juga mendorong terciptanya budaya digital yang lebih aman dan bertanggung jawab di kalangan masyarakat, khususnya di lingkungan LKP Mutiara Informatika. Dengan bekal pengetahuan yang diberikan, diharapkan peserta mampu menerapkan langkah-langkah perlindungan data secara mandiri serta menjadi agen literasi digital yang dapat menyebarkan pemahaman tersebut ke lingkungan sekitar.

### UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, kami mengucapkan terima kasih yang sebesar-besarnya kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Royal atas dukungan, bimbingan, serta fasilitasi yang telah diberikan sehingga kegiatan Pengabdian kepada Masyarakat dan Ucapan terima kasih juga kami sampaikan kepada LKP Mutiara Informatika sebagai mitra pelaksana kegiatan, atas kerja sama yang luar biasa, serta kesediaannya menjadi tempat berlangsungnya pelatihan ini. Partisipasi aktif dari peserta dan dukungan dari seluruh tim di LKP Mutiara Informatika sangat membantu dalam menyukseskan program ini.

### DAFTAR PUSTAKA

Adma, A., Indonesia, U., & Sari, P. (2023). Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber

Mandiri di Masa Depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, 6(1).  
<https://doi.org/10.7454/jkskn.v6i1.10077>

Ghalib, Y. W., Gilang, E. F., Zumi M, Abdhe F, Nanda A, Serly D A, & Zurkiyah A. (2024). Analisis Perkembangan Keamanan Siber Dampak Dari Kebocoran Data Pusat Data Nasional Sementara 2 Surabaya Assessing And Understanding The Current Situation: Analysis Of Cyber Security Developments The Impact Of The Temporary National Data Center Data Leaks 2 Surabaya Oleh. *JISCO (Journal of Informaaoon System and Compuung)* ISSN, 2(June).

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM*, 3(03), 118–124.  
<https://doi.org/10.58812/shh.v3i03.544>

Na, G. (2025). *Data Security Governance Practices under the Background of AI Era*. 5(5), 11–15.

Sulubara, S. M. (2024). Pencurian Data dan Peretasan Situs Web Pemerintah. *Hukum Dan Ilmu Komunikasi*, 1(6), 199–206.  
<https://journal.appisi.or.id/index.php/konsensus>

Tommy, S., & Nasution, M. I. P. (2025). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN). *Jurnal Ilmiah Ekonomi Dan Manajemen*, 3(6), 330–346.