

## **Keamanan Data Pribadi di Ruang Digital: Edukasi dan Literasi Ancaman Siber**

**Riad Sahara<sup>1\*</sup>, Cian Ramadhona Hassolthine<sup>2</sup>, Syahid Abdullah<sup>3</sup>, Catur Nugroho<sup>4</sup>,  
 Ambros Magnus Rudolf Mekeng<sup>5</sup>, Muhammad Ikhwan Saputra<sup>6</sup>**

<sup>1,2,3,4,5,6</sup>Universitas Siber Asia

Email: riadsahara@lecturer.unsia.ac.id

*Received: 02-08-2026    Revised : 17-08-2026    Accepted : 22-08-2026    Published : 26-08-2026*

### **Abstrak**

Kemudahan dalam memperoleh, menyebarkan, dan menyimpan informasi melalui internet memberikan berbagai manfaat bagi masyarakat, termasuk dalam aktivitas komunikasi, finansial, dan *e-commerce*. Di sisi lain, penggunaan teknologi digital menghadirkan risiko pelanggaran privasi, pencurian data pribadi, kebocoran data, serta penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Kondisi tersebut menegaskan pentingnya literasi keamanan data agar masyarakat mampu memahami dan mengantisipasi berbagai risiko dalam aktivitas digital. Kegiatan Pengabdian kepada Masyarakat (PKM) ini bertujuan meningkatkan pemahaman peserta mengenai perlindungan data pribadi, mengenali ancaman *phishing* dan *social engineering*, serta menerapkan langkah dasar keamanan data dalam aktivitas digital sehari-hari. Kegiatan dilaksanakan secara luring melalui seminar yang terdiri atas pemaparan materi dan diskusi interaktif. Materi mencakup tren kebocoran data, keamanan data pribadi, CIA Triad, pola *social engineering*, karakteristik *phishing*, serta langkah pencegahan dan perlindungan data pribadi di internet. Kegiatan memberikan pemahaman praktis kepada peserta mengenai pola ancaman siber dan langkah dasar dalam menjaga keamanan informasi pribadi. Peserta memperoleh pengetahuan untuk lebih berhati-hati dalam menyimpan dan membagikan informasi pribadi, mengenali indikasi pesan atau tautan *phishing*, serta menerapkan perlindungan dasar terhadap akun dan data pribadi. Evaluasi kuantitatif melalui *pre-test* dan *post-test* belum diterapkan dalam kegiatan ini, sehingga capaian program disajikan berdasarkan pelaksanaan edukasi dan keterlibatan peserta dalam sesi diskusi. Kegiatan ini memperkuat pentingnya edukasi keamanan data pribadi sebagai langkah membangun kesadaran dan perilaku digital yang lebih aman.

**Kata kunci:** keamanan data pribadi, keamanan siber, literasi digital, phishing, perlindungan data pribadi

### **Abstract**

*The ease of accessing, disseminating, and storing information through the internet provides various benefits to society, including communication, financial activities, and e-commerce. At the same time, the use of digital technology creates risks related to privacy violations, personal data theft, data breaches, and the misuse of information by irresponsible parties. These conditions emphasize the importance of data security literacy to enable individuals to understand and anticipate risks associated with digital activities. This Community Service Program (PKM) aimed to strengthen participants' understanding of personal data protection,*

*recognize phishing and social engineering threats, and apply basic data security practices in everyday digital activities. The program was conducted offline through a seminar consisting of material presentations and interactive discussions. The topics covered data breach trends, personal data security, the CIA Triad, social engineering patterns, common characteristics of phishing, and preventive measures for protecting personal data on the internet. The activity provided participants with practical knowledge of cyber threat patterns and basic measures for safeguarding personal information. Participants gained knowledge on exercising greater caution when storing and sharing personal information, recognizing indications of phishing messages or links, and applying basic protection to their accounts and personal data. Quantitative evaluation through pre-test and post-test assessments was not implemented; therefore, program outcomes are presented based on the educational activities and participants' engagement during the discussion sessions. This program reinforces the importance of personal data security education as a foundation for developing greater awareness and safer digital practices.*

**Keywords:** *cybersecurity, digital literacy, personal data protection, personal data security, phishing*

## Pendahuluan

Kemajuan perkembangan teknologi internet dan penyebaran informasi membawa perubahan yang signifikan dalam aktivitas masyarakat, terutama dalam cara berkomunikasi serta beberapa proses bisnis. Kemudahan dalam memperoleh informasi, menyebarluaskan informasi, menyimpan informasi dalam media digital ataupun media sosial yang diakses melalui jaringan internet merupakan satu dari sekian banyak keuntungan yang bisa dirasakan dari kemajuan tersebut (Betty Yel & M Nasution, 2022; Lesmana et al., 2022; Yuniarti, 2019). Keuntungan lainnya bisa dirasakan dalam proses bisnis yang berhubungan dengan finansial, *e-commerce*, pendidikan, dan proses bisnis lainnya. Saat ini penggunaan kedua produk teknologi informasi tersebut memang sedang meningkat pesat karena kemudahan penggunaan dan proses yang ditawarkan dengan memanfaatkan kemajuan teknologi yang ada (Kesuma et al., 2021; Poeja Kehista et al., 2023).

Dari pesatnya perkembangan kemajuan teknologi internet dan penyebaran informasi melalui media internet, selain mendatangkan banyak hal positif atau keuntungan yang bisa kita rasakan, tetapi juga tidak dapat dipungkiri ada beberapa dampak negatif atau kerugian yang harus diperhatikan dan ditanggulangi dengan tepat. Kasus-kasus mengenai pelanggaran privasi individu, pencurian data pribadi, kebocoran data personal atau pribadi, hingga penyalahgunaan data personal oleh oknum yang tidak bertanggungjawab menjadi dampak negatif atau masalah utama yang muncul (Betty Yel & M Nasution, 2022; Ginanjar & Lubis, 2022; Kesuma et al., 2021; Lesmana et al., 2022; Poeja Kehista et al., 2023; Rumlus & Hartadi, 2020; Yuniarti, 2019). Kejadian seperti ini memang sudah merupakan hal yang pasti akan terjadi dalam *cyber space* (Ginanjar & Lubis, 2022). Semakin terasa dampak negatif yang akan dirasakan karena sampai saat ini di Indonesia sendiri memang masih belum adanya undang-undang atau peraturan khusus untuk menangani kasus atas pelanggaran data pribadi (Rumlus & Hartadi, 2020).

Kebutuhan kegiatan diarahkan pada penguatan pemahaman masyarakat mengenai bentuk-bentuk ancaman terhadap data pribadi yang sering muncul dalam aktivitas digital. Pemahaman mengenai kebocoran data, pola *social engineering*, karakteristik *phishing*, serta langkah dasar perlindungan informasi pribadi menjadi aspek penting agar pengguna internet mampu mengenali risiko sebelum memberikan, menyimpan, atau menyebarluaskan data pribadinya. Kebutuhan tersebut menunjukkan bahwa edukasi keamanan data tidak cukup hanya menjelaskan pentingnya menjaga privasi, tetapi juga perlu memberikan pemahaman praktis mengenai pola ancaman dan cara meresponsnya secara tepat.

Edukasi dan *literasi* mengenai keamanan data pribadi menjadi bagian penting dalam membangun kesadaran masyarakat terhadap risiko penggunaan teknologi digital. Perlindungan data pribadi tidak hanya berkaitan dengan upaya menjaga informasi yang bersifat rahasia, tetapi juga dengan kemampuan individu mengenali potensi kebocoran data, memahami pola serangan, serta menerapkan langkah pencegahan dalam aktivitas digital sehari-hari. Kepedulian terhadap keamanan data pribadi yang disimpan di internet juga hal yang utama perlu ditingkatkan agar terhindar dari kerugian-kerugian yang mengancam atas dampak negatif dari perkembangan kemajuan teknologi internet dan penyebaran informasi. Melalui program Pengabdian kepada Masyarakat (PKM), peserta diberikan edukasi yang mengintegrasikan pemahaman mengenai *data breach*, konsep CIA Triad, *social engineering*, *phishing*, serta langkah perlindungan data pribadi dalam satu rangkaian pembelajaran. Integrasi materi tersebut menjadi karakter khusus kegiatan karena peserta tidak hanya memperoleh informasi mengenai risiko keamanan data, tetapi juga diperkenalkan pada pola terjadinya ancaman dan langkah praktis untuk mengantisipasinya.

Solusi yang diterapkan dalam kegiatan ini berupa edukasi keamanan data pribadi yang disusun secara bertahap, mulai dari pengenalan tren dan kasus kebocoran data, pemahaman prinsip dasar keamanan informasi melalui CIA Triad, pengenalan pola *social engineering* dan *phishing*, hingga pembahasan mengenai langkah perlindungan data pribadi di internet. Peserta juga diperkenalkan dengan contoh dan simulasi pola pencurian serta pelanggaran data agar mampu memahami bagaimana ancaman dapat terjadi dalam aktivitas digital. Dengan pendekatan tersebut, kegiatan ini bertujuan memperkuat pemahaman peserta mengenai perlindungan data pribadi, meningkatkan kewaspadaan terhadap ancaman siber, serta mendorong penerapan langkah dasar keamanan data dalam penggunaan internet sehari-hari.

## Metode

Kegiatan Pengabdian kepada Masyarakat (PKM) dilaksanakan secara luring melalui skema seminar yang dirancang untuk memberikan edukasi mengenai keamanan data pribadi dan berbagai risiko yang muncul dalam aktivitas digital. Kegiatan diarahkan pada pemberian pemahaman konseptual dan praktis kepada peserta agar mampu mengenali bentuk ancaman terhadap data pribadi serta memahami langkah dasar yang dapat diterapkan untuk menjaga keamanan informasi ketika menggunakan internet dan layanan digital.

Pelaksanaan kegiatan terdiri atas dua tahap utama. Tahap pertama berupa pemaparan materi mengenai keamanan data pribadi, tren kebocoran data, prinsip dasar keamanan informasi, pola ancaman siber, serta langkah perlindungan data. Tahap kedua berupa diskusi dan tanya jawab yang memberikan kesempatan kepada peserta untuk mengaitkan materi dengan permasalahan keamanan data yang dijumpai dalam aktivitas digital sehari-hari. Materi

kegiatan dikelompokkan ke dalam empat tema utama agar proses edukasi berlangsung secara sistematis, sebagaimana disajikan pada Tabel 1.

Tabel 1. Materi PKM *Personal Data Security Awareness*

| No. | Tema Utama                                  | Materi Pembahasan                                                                                                                                                                                                                                                                                         | Tujuan Pembelajaran                                                                                                                                                                       |
|-----|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Tren dan Risiko Kebocoran Data              | Literasi keamanan data pribadi; <i>most-breached countries</i> ; <i>timeline of the biggest data breaches</i> ; status kebocoran data Indonesia 2024; kasus kebocoran data perusahaan di Indonesia; empat kasus kebocoran data di Indonesia tahun 2023; serta contoh pemeriksaan kebocoran data personal. | Memberikan pemahaman kepada peserta mengenai perkembangan kasus kebocoran data dan berbagai risiko yang dapat muncul ketika data pribadi tersimpan atau dibagikan melalui media digital.  |
| 2   | Konsep Dasar Perlindungan Data Pribadi      | Pelanggaran atau kebocoran data, siklus pelanggaran data, CIA Triad, serta alasan pentingnya perlindungan data pribadi.                                                                                                                                                                                   | Memberikan pemahaman mengenai prinsip kerahasiaan, integritas, dan ketersediaan informasi serta keterkaitannya dengan perlindungan data pribadi.                                          |
| 3   | Pengenalan Ancaman dan Langkah Perlindungan | Cara melindungi data pribadi di internet, pola <i>social engineering</i> , cara mengenali dan menghindari serangan <i>phishing</i> , serta indikator umum dalam upaya <i>phishing</i> .                                                                                                                   | Membekali peserta dengan pengetahuan dasar untuk mengenali pola ancaman siber serta memahami langkah pencegahan dalam penggunaan layanan digital.                                         |
| 4   | Diskusi dan Penerapan Praktis               | Diskusi, tanya jawab, pembahasan contoh kasus, serta pengaitan materi keamanan data dengan aktivitas digital peserta.                                                                                                                                                                                     | Memberikan ruang kepada peserta untuk mengklarifikasi materi, membahas permasalahan yang ditemui, serta memahami penerapan langkah perlindungan data pribadi dalam aktivitas sehari-hari. |

Pada tahap pemaparan, peserta diperkenalkan dengan tren dan kasus kebocoran data, konsep CIA Triad, pola *social engineering* dan *phishing*, serta langkah perlindungan data pribadi. Penyampaian materi dilengkapi dengan contoh kasus dan simulasi pola pencurian serta pelanggaran data untuk memberikan gambaran mengenai bagaimana ancaman terhadap informasi pribadi dapat terjadi dalam aktivitas digital.

Tahap berikutnya dilaksanakan melalui diskusi dan tanya jawab. Pada tahap ini, peserta diberikan kesempatan untuk mengajukan pertanyaan, mendiskusikan situasi yang berkaitan dengan keamanan data pribadi, serta menghubungkan materi yang telah disampaikan dengan penggunaan internet dalam kehidupan sehari-hari. Tahap ini sekaligus

digunakan untuk memperkuat pemahaman peserta mengenai identifikasi ancaman dan langkah dasar perlindungan data pribadi.

## Hasil

Kegiatan PKM telah dilaksanakan dalam skema seminar berupa penyampaian materi 100% yang akan memakan waktu kurang lebih 1 hari jam kerja yang meliputi:

### Tahap I: Presentasi (Pemaparan Materi)

Pada tahap pertama penyelenggaraan PKM peserta akan dibekali dengan literasi tentang tren keamanan data saat ini, serta teori atau informasi bagaimana cara mengamankan data pribadi di internet. Kemudian pemateri memberikan motivasi untuk meningkatkan kepedulian dalam mengamankan data pribadi yang disimpan di internet seperti yang ditunjukkan pada Gambar 1 berikut ini.



Gambar 1. Dokumentasi Pelaksanaan PKM *Personal Data Security Awareness* (Dokumentasi Penulis dari hasil kegiatan)

Mengapa pengetahuan mengenai tren keamanan data pribadi ini penting? Hal ini untuk menunjukkan kepada masyarakat berapa banyak data pribadi yang sudah bocor, kenapa data pribadi bisa bocor, apa dampak jika data pribadi bocor, dan sebagainya. Pelanggaran data atau kebocoran data adalah pelepasan data sensitif, rahasia, atau dilindungi ke lingkungan yang tidak terpercaya (Sukmawan & Setyawan, 2023). Pelanggaran data dapat terjadi sebagai akibat dari serangan peretas, pekerjaan orang dalam yang dilakukan oleh individu yang saat ini atau sebelumnya bekerja di suatu organisasi, atau kehilangan atau paparan data yang tidak disengaja (Hidayatullah, 2023). Berdasarkan hasil riset dari salah satu perusahaan *cybersecurity* di global, menunjukkan di Indonesia sendiri pada tahun 2024 sudah terjadi kebocoran data sebanyak lebih dari 157 juta data dari total lebih dari 17 milyar data secara global (Surfshark, 2024) seperti yang ditunjukkan seperti pada gambar 2 di bawah ini.

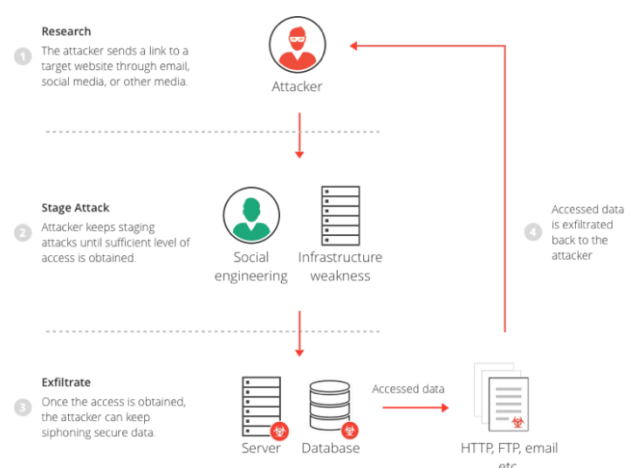


Gambar 2. Data Breach Map (Surfshark, 2024).

Setelah pemaparan awal dan pengenalan materi mengenai tren keamanan data pribadi, masyarakat lebih memahami mengapa data pribadi penting untuk dilindungi dan apa akibatnya jika abai terhadap hal tersebut. Berikut ini beberapa alasan mengapa data personal atau data pribadi sangat penting untuk dilindungi (CNN Indonesia, 2019):

1. Menghindari adanya upaya intimidasi terkait gender yang dilakukan secara *online*;
2. Mencegah penyalahgunaan data pribadi atau data personal yang dapat dilakukan pihak yang tidak bertanggungjawab;
3. Meminimalisir menjadi korban penipuan secara *online*;
4. Menghindari terjadinya potensi pencemaran nama baik; dan
5. Memberikan hak kendali dari data personal atau data pribadi.

Selain itu masyarakat juga diperkenalkan sekaligus disimulasikan mengenai model serta alur dari pencurian dan pelanggaran data pribadi melalui serangan yang umum terjadi seperti *Social Engineering attack* seperti pada Gambar 3 berikut ini.



Gambar 3. *Example of data breach attack cycle* (Imperva, 2024)

Setelah mendapatkan pengetahuan tentang tren keamanan data secara umum, tren kebocoran dan pencurian data pribadi, lalu contoh-contoh kasus yang terjadi, bagaimana cara

menyikapi dan menanggulangi hal-hal tersebut, diharapkan masyarakat lebih memahami betapa pentingnya untuk memperhatikan keamanan data pribadi, khususnya data-data pribadi yang tersimpan di internet.

## **Tahap II: Diskusi (Tanya Jawab)**

Tahap kedua dilaksanakan melalui sesi diskusi dan tanya jawab setelah seluruh materi utama disampaikan. Sesi ini memberikan ruang kepada peserta untuk mengklarifikasi materi serta mengaitkan konsep keamanan data dengan situasi yang dapat dijumpai dalam aktivitas digital sehari-hari. Pembahasan diarahkan pada risiko kebocoran data, pola *social engineering*, identifikasi *phishing*, serta langkah yang dapat dilakukan ketika menghadapi indikasi ancaman terhadap informasi pribadi.

Diskusi menjadi bagian penting dalam kegiatan karena peserta tidak hanya menerima materi secara satu arah, tetapi juga memperoleh kesempatan untuk membahas penerapan perlindungan data dalam konteks penggunaan internet. Interaksi pada tahap ini digunakan untuk memperkuat kembali pemahaman mengenai pentingnya kehati-hatian dalam memberikan informasi pribadi, mengenali komunikasi digital yang mencurigakan, serta menerapkan langkah dasar perlindungan data. Dengan demikian, capaian kegiatan tidak hanya berupa tersampainya materi, tetapi juga tersedianya ruang interaktif untuk menghubungkan pengetahuan keamanan data dengan praktik penggunaan teknologi digital.

## **Pembahasan**

Pelaksanaan kegiatan Pengabdian kepada Masyarakat mengenai *Personal Data Security Awareness* menunjukkan relevansi edukasi keamanan data pribadi dalam membekali peserta dengan pengetahuan mengenai berbagai risiko yang muncul dalam aktivitas digital. Materi mengenai tren kebocoran data, bentuk pelanggaran data, *social engineering*, *phishing*, CIA Triad, serta cara melindungi data pribadi memberikan pemahaman bahwa keamanan data tidak hanya menjadi tanggung jawab penyedia layanan digital, tetapi juga membutuhkan kepedulian dari setiap pengguna. Hal ini sejalan dengan Betty Yel dan M Nasution (2022), Ginanjar dan Lubis (2022), serta Poeja Kehista et al. (2023) yang menekankan pentingnya perlindungan data pribadi karena meningkatnya risiko penyalahgunaan, pencurian, dan kebocoran data dalam penggunaan layanan berbasis internet (Betty Yel & M Nasution, 2022; Ginanjar & Lubis, 2022; Poeja Kehista et al., 2023).

Pendekatan edukasi yang menggabungkan penjelasan konseptual, contoh kasus, dan pengenalan ancaman *phishing* juga memiliki dasar empiris dari penelitian terdahulu. Khan et al. (2023) menunjukkan bahwa pelatihan kesadaran keamanan siber mampu meningkatkan pengetahuan peserta mengenai ancaman dan strategi penanggulangannya serta memperkuat *self-efficacy* dalam menerapkan perilaku keamanan siber. Temuan Ismail et al. (2023) juga memperlihatkan peningkatan skor kesadaran peserta setelah mengikuti program edukasi *phishing* yang memadukan materi pembelajaran dengan evaluasi sebelum dan sesudah kegiatan. Selain itu, Sarker et al. (2024), melalui kajian terhadap berbagai program edukasi dan pelatihan *phishing*, menegaskan bahwa keberhasilan edukasi keamanan siber perlu mempertimbangkan kesenjangan pengetahuan pengguna, faktor manusia, dan bentuk pembelajaran yang sesuai dengan karakteristik peserta. Temuan-temuan tersebut memperkuat pendekatan kegiatan ini yang tidak hanya memperkenalkan ancaman secara umum, tetapi

mengintegrasikan *data breach*, CIA Triad, *social engineering*, *phishing*, dan langkah perlindungan data pribadi dalam satu rangkaian edukasi.

Penyampaian materi yang dilanjutkan dengan diskusi juga memberikan ruang bagi peserta untuk mengaitkan konsep keamanan data dengan aktivitas digital sehari-hari. Pembahasan mengenai pola serangan, indikator *phishing*, serta contoh *social engineering* memberikan konteks praktis bagi peserta untuk mengenali kondisi yang berpotensi mengancam keamanan informasi pribadi. Pendekatan berbasis contoh dan simulasi juga relevan dengan Hillman et al. (2023), yang menegaskan bahwa kesadaran pengguna dan perilaku proaktif tetap menjadi komponen penting dalam menghadapi serangan *phishing*. Dengan demikian, edukasi keamanan siber perlu diarahkan tidak hanya pada pengetahuan mengenai ancaman, tetapi juga pada kemampuan pengguna untuk mengenali dan merespons situasi berisiko dalam aktivitas digital.

Pemahaman terhadap pola serangan dan langkah pencegahan diharapkan dapat mendorong peserta lebih berhati-hati dalam menyimpan, membagikan, dan mengelola informasi pribadi di internet. Implikasi praktis kegiatan ini terletak pada pembentukan dasar kewaspadaan digital, terutama dalam mengenali pesan atau tautan yang mencurigakan, membatasi pemberian informasi pribadi kepada pihak yang tidak terverifikasi, serta memahami pentingnya menjaga kerahasiaan dan integritas data. Evaluasi kuantitatif melalui *pre-test* dan *post-test* belum diterapkan dalam kegiatan ini sehingga perubahan tingkat literasi peserta belum dinyatakan dalam bentuk skor. Pengembangan kegiatan selanjutnya perlu memasukkan evaluasi sebelum dan sesudah edukasi serta simulasi berbasis kasus untuk mengukur perubahan pengetahuan dan kemampuan peserta dalam mengidentifikasi ancaman secara lebih objektif. Pendekatan tersebut juga penting untuk menilai keberlanjutan hasil edukasi, mengingat Sikolia et al. (2023) menemukan bahwa pelatihan kesadaran keamanan dapat meningkatkan pengetahuan dan menurunkan kerentanan terhadap *phishing*, tetapi sebagian peningkatan pengetahuan dapat menurun kembali seiring waktu.

Kegiatan ini juga memiliki relevansi dengan kerangka hukum perlindungan data pribadi di Indonesia. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menempatkan pelindungan data pribadi sebagai bagian dari pelindungan diri pribadi dan diarahkan untuk menjamin hak warga negara sekaligus menumbuhkan kesadaran masyarakat mengenai pentingnya pelindungan data pribadi. Dalam konteks tersebut, edukasi mengenai kebocoran data, *social engineering*, *phishing*, dan langkah perlindungan informasi pribadi menjadi bentuk penguatan literasi masyarakat untuk mendukung perilaku pengelolaan data yang lebih aman. Program ini tidak hanya relevan dari sisi teknis keamanan siber, tetapi juga mendukung pemahaman masyarakat mengenai hak, tanggung jawab, dan kehati-hatian dalam pemrosesan serta penggunaan data pribadi di ruang digital.

## Kesimpulan

Kegiatan Pengabdian kepada Masyarakat mengenai *Personal Data Security Awareness* telah memberikan edukasi kepada peserta mengenai tren keamanan data, risiko kebocoran dan penyalahgunaan data pribadi, *social engineering*, *phishing*, CIA Triad, serta langkah dasar perlindungan data pribadi di internet. Rangkaian pemaparan materi, studi kasus, simulasi, dan diskusi memberikan dasar pemahaman kepada peserta untuk mengenali berbagai bentuk

ancaman siber serta menerapkan sikap yang lebih berhati-hati dalam menyimpan, membagikan, dan mengelola informasi pribadi dalam aktivitas digital. Kegiatan ini juga menegaskan bahwa perlindungan data pribadi membutuhkan peran aktif setiap pengguna, terutama dalam menjaga informasi yang berkaitan dengan identitas, bisnis, finansial, dan data sensitif lainnya.

Kegiatan selanjutnya perlu dikembangkan melalui edukasi keamanan data yang dilakukan secara berkelanjutan dan lebih berorientasi pada praktik. Simulasi *phishing* dan *social engineering* dapat digunakan untuk melatih kemampuan peserta dalam mengenali pola serangan secara langsung. Materi juga perlu diperkuat dengan praktik penggunaan autentikasi berlapis atau *multi-factor authentication*, pengelolaan kata sandi yang aman, serta langkah perlindungan akun digital. Evaluasi terhadap perilaku keamanan digital peserta perlu dilakukan untuk menilai penerapan pengetahuan dalam aktivitas sehari-hari, disertai evaluasi sebelum dan sesudah kegiatan untuk memperoleh gambaran capaian program secara lebih terukur.

### Daftar Pustaka

- Betty Yel, M., & M Nasution, M. K. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, 6(1), 92–101. <https://doi.org/10.59697/jik.v6i1.144>
- CNN Indonesia. (2019, July 15). 5 Alasan Mengapa Data Pribadi Perlu Dilindungi. <https://www.cnnindonesia.com/teknologi/20190715201531-185-412391/5-alasan-mengapa-data-pribadi-perlu-dilindungi>
- Ginanjari, D., & Lubis, A. F. (2022). Urgensi Perlindungan Data Pribadi Dalam Menjamin Keamanan Data. *Jurnal Hukum Dan HAM West Science*, 01(01), 21–26. <https://doi.org/https://doi.org/10.58812/jhhws.v1i01.7>
- Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding SAINTEK: Sains Dan Teknologi*, 2(1), 216–221.
- Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, 132, 103364. <https://doi.org/10.1016/j.cose.2023.103364>
- Imperva. (2024). *What is a Data Breach | Tips for Data Leak Prevention | Imperva*. <https://www.imperva.com/learn/data-security/data-breach/>
- Ismail, N. N. S., Fammy Rikzan, F. I., Katuk, N., Hashim, N. L., & Mohd Zulkefli, N. A. (2023). Enhancing information security awareness on phishing among IT students: A pilot test case study at Politeknik Tuanku Syed Sirajuddin. *Journal of Digital System Development*, 1, 12–23. <https://doi.org/10.32890/jdsd2023.1.2>
- Kesuma, A. A. N. D. H., Budiarta, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik. *Jurnal Preferensi Hukum*, 2(2), 411–416. <https://doi.org/10.22225/jph.2.2.3350.411-416>
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, 125, 103049. <https://doi.org/10.1016/j.cose.2022.103049>

- Lesmana, C. T., Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia. *JURNALRECHTEN:RISETHUKUMDANHAKASASIMANUSIA*, 3(2), 1–6. <https://doi.org/https://doi.org/10.52005/rechten.v3i2.78>
- Poeja Kehista, A., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan (JIMT)*, 4(5), 625–632. <https://doi.org/10.31933/jimt.v4i5>
- Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
- Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, 11(2), 285. <https://doi.org/10.30641/ham.2020.11.285-299>
- Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*, 208, 111899. <https://doi.org/10.1016/j.jss.2023.111899>
- Sikolia, D., Biros, D., & Zhang, T. (2023). How effective are SETA programs anyway: Learning and forgetting in security awareness training. *Journal of Cybersecurity Education, Research and Practice*, 2023(1).
- Sukmawan, D. I., & Setyawan, D. P. (2023). Peretas, Ketakutan, dan Kerugian: Pelanggaran Data dan Keamanan Nasional. *Global Strategis*, 17(1).
- Surfshark. (2024, July 15). *Data breach statistics globally - Surfshark*. <https://surfshark.com/research/data-breach-monitoring>
- Yuniarti, S. (2019). PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA. *Business Economic, Communication, and Social Sciences*, 1(1), 147–154.