

## Edukasi Keamanan Cyber Kepada Masyarakat Dari Ancaman Digital

Hario Jati Setyadi<sup>1,\*</sup>, Amin Padmo Azam Masa<sup>2</sup>, Putut Pamilih Widagdo<sup>3</sup>, Akhmad Irsyad<sup>4</sup>, Sandrina Aulia<sup>5</sup>, Muhammad Hisyam Nugroho<sup>6</sup>, Nazwa Tri Ananda<sup>7</sup>

<sup>1,2,3,4,5,6,7</sup>Program Studi Sistem Informasi, Fakultas Teknik, Universitas Mulawarman  
E-Mail : hariojati.setyadi@unmul.ac.id <sup>1</sup>; aminpadmo@unmul.ac.id <sup>2</sup>; putut@unmul.ac.id <sup>3</sup>;  
akhmadirsyad@unmul.ac.id <sup>4</sup>; sndrnaa24@gmail.com <sup>5</sup>; nmuhammadhisyam@gmail.com <sup>6</sup>;  
nazwatrianand@gmail.com <sup>7</sup>

### ABSTRAK

Kegiatan ini merupakan pengabdian masyarakat yang dilaksanakan di Kelurahan Tanah Merah, Kecamatan Samarinda Utara, yang mengambil tema Masyarakat Desa Tanah Merah, yaitu kawasan strategis dan kaya akan potensi sumber daya alam dan budaya. Kelurahan ini terletak di daerah perbukitan dan memiliki banyak mata air yang menjadi sumber irigasi utama bagi daerah sekitarnya. Tanah Merah sebagian besar dihuni oleh masyarakat yang bergerak di bidang pertanian, peternakan, dan kerajinan tangan. Mereka mengolah hasil pertanian seperti sayuran dan buah-buahan dan menjualnya di berbagai pasar lokal di Samarinda dan sekitarnya. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan pemahaman tentang keamanan siber di Kelurahan Tanah Merah, Samarinda. Masalah utama yang dihadapi masyarakat adalah rendahnya kesadaran akan pentingnya melindungi data pribadi di tengah tingginya ancaman digital. Metode yang digunakan dalam kegiatan ini meliputi edukasi lisan, demonstrasi praktik keamanan digital dan pendekatan interaktif partisipatif-kolaboratif. Pada hari pelaksanaan masyarakat diberikan materi tentang jenis ancaman siber termasuk *phishing* dan *malware*, serta cara melindungi data menggunakan fitur keamanan pada perangkat digital. Hasil evaluasi menunjukkan peningkatan pemahaman masyarakat mengenai keamanan digital diukur melalui *pre-test* dan *post-test* yang mencakup pemahaman konsep dan keterampilan praktik. Partisipasi aktif masyarakat pada sesi tanya jawab mengindikasikan antusiasme serta kesadaran yang lebih baik terhadap pentingnya perlindungan data pribadi. Dampak kegiatan ini berupa perubahan perilaku dalam penggunaan teknologi digital secara aman serta keinginan masyarakat untuk terus mendapatkan edukasi berkelanjutan. Dengan demikian, kegiatan ini berhasil menciptakan landasan penting bagi penguatan keamanan siber di tingkat masyarakat lokal.

Kata Kunci – Ancaman Digital, Data Pribadi, Edukasi Digital, Keamanan Siber, Masyarakat.

### ABSTRACT

*This community service program was carried out in Tanah Merah Village, North Samarinda District, embracing the theme of Tanah Merah Village as a strategic area rich in natural and cultural resources. The village, located in hilly terrain with abundant springs that serve as the primary irrigation source for surrounding areas, is largely inhabited by communities engaged in agriculture, livestock, and handicrafts. They process agricultural products like vegetables and fruits, selling them in local markets around Samarinda and its vicinity. This community service program aims to enhance understanding of cybersecurity in Tanah Merah Village, Samarinda. The main issue faced by the community is the low awareness of the importance of protecting personal data amid increasing digital threats. The methods used in this activity include verbal education, practical demonstrations of digital security and a participative-collaborative approach. On the day of implementation, the community was provided with material on types of cyber threats, including phishing and malware and ways to protect data using security features on digital devices. Evaluation results showed an increase in the community's understanding of digital security, measured through pre-test and post-test assessments covering conceptual understanding and practical skills. The active participation of the community in the question-and-answer session indicated enthusiasm and a greater awareness of the importance of personal data protection. The impact of this activity includes behavioral changes in the safe use of digital technology and a desire for ongoing education. Thus, this program successfully lays a critical foundation for strengthening cybersecurity at the local community level.*

Keywords – Community, Cybersecurity, Digital Education, Digital Threats, Personal Data.

---

\*) Corresponding Author

## 1. PENDAHULUAN

Pengembangan keamanan siber dan kedaulatan data di negara-negara termasuk Indonesia membuat perlindungan data pribadi setiap warga penting. Dalam hal ini, hak setiap warga negara untuk memiliki kemampuan untuk menjaga data pribadi mereka dan mendapatkan jaminan perlindungan negara agar merasa "aman" dan "bebas" di internet (Wulansari, 2020). Dalam beberapa tahun terakhir, Indonesia mengalami serangkaian insiden kebocoran data yang signifikan. Pada Juni 2024, Pusat Data Nasional (PDN) mengalami serangan siber yang mengakibatkan gangguan pada layanan pemerintah, termasuk pemeriksaan imigrasi di bandara. Pelaku serangan menuntut tebusan sebesar 8 juta dolar AS, menggunakan ransomware Lockbit 3.0 (Widiyanto & Ananda, 2024). Sebelumnya, pada Mei 2023, Bank Syariah Indonesia (BSI) menjadi korban serangan ransomware oleh grup LockBit, yang mengklaim telah menyebarkan data sebesar 1,5 terabit ke pasar gelap internet (Akbar, 2024). Selain itu, pada Juli 2023, dilaporkan bahwa 337 juta data dari Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri bocor, mencakup informasi pribadi seperti NIK hingga nomor akta lahir atau nikah (Setiawan, 2023).

Indonesia menghadapi tantangan keamanan siber yang serius termasuk kebocoran data dan ancaman digital lainnya yang berdampak pada berbagai sektor tidak hanya pada sektor swasta tapi juga pada sektor pemerintahan. Masyarakat di Kelurahan Tanah Merah, Kecamatan Samarinda Utara menghadapi bahaya yang sama yakni kurang memahami lebih dalam terkait keamanan digital. Badan Siber dan Sandi Negara (BSSN) mencatat 207 kebocoran data di tahun 2023, dengan 55% diantaranya terjadi di sektor pemerintahan menunjukkan bahwa keamanan siber perlu ditingkatkan (Septiani, 2023). Kelurahan Tanah Merah yang terletak di Kecamatan Samarinda Utara Kota Samarinda dikenal sebagai kawasan strategis dan kaya akan potensi sumber daya alam dan budaya. Kelurahan ini terletak di daerah perbukitan dan memiliki banyak mata air yang menjadi sumber irigasi utama bagi daerah sekitarnya. Tanah Merah sebagian besar dihuni oleh masyarakat yang bergerak di bidang pertanian, peternakan, dan kerajinan tangan. Mereka mengolah hasil pertanian seperti sayuran dan buah-buahan dan menjualnya di berbagai pasar lokal di Samarinda dan sekitarnya. Selain itu, kelurahan atau bisa dianggap sebagai Desa Tanah Merah ini juga terkenal dengan kerajinan anyaman rotan dan bambu yang dibuat oleh sekelompok perajin setempat. Anyaman ini tidak hanya memiliki nilai estetika yang tinggi, namun juga mendukung kelestarian lingkungan karena penggunaan bahan baku alami lokal.

Kelurahan ini telah lama dikenal sebagai lokasi wisata alam dengan pemandangan yang masih asri dan sejuk. Keindahan perbukitan dan mata air yang bersih menjadikannya daya tarik tersendiri bagi wisatawan yang mencari suasana tenang. Pemerintah setempat bekerja sama dengan masyarakat mengembangkan Tanah Merah sebagai desa wisata dengan konsep ekowisata yang fokus pada perlindungan lingkungan dan pengembangan industri kreatif. Wisatawan yang berkunjung ke Desa Tanah Merah tidak hanya menikmati keindahan alam, namun juga mengikuti kegiatan edukasi seperti mempelajari proses pembuatan anyaman dan cara menanam produk pertanian secara organik. Hal ini merupakan salah satu upaya pemerintah dan masyarakat untuk meningkatkan perekonomian masyarakat. Aktivitas Masyarakat saat ini semakin beralih dari aktivitas konvensional ke aktivitas yang dilakukan di dunia virtual. Aplikasi seperti *WhatsApp*, *Facebook*, *Instagram*, *Twitter*, *TikTok*, dan lainnya sudah menjadi bagian integral dari kehidupan masyarakat (Arham, M. R. H., & Risal, M. C., 2023). Pemerintah dan masyarakat harus meningkatkan kesadaran keamanan siber. Banyak masyarakat yang menggunakan perangkat seperti smartphone dan laptop setiap hari, tetapi mereka tidak tahu cara melindungi data dan privasi mereka dari serangan internet. Ancaman seperti *phishing*, *malware*, dan pencurian identitas semakin meningkatkan risiko, terutama dengan meningkatnya akses terhadap teknologi yang digunakan tanpa pemahaman tentang praktik online yang aman. Masyarakat tidak mampu melindungi diri mereka dari ancaman-ancaman ini, sehingga menjadikan mereka lebih rentan, terutama ketika dihadapkan pada ancaman-ancaman yang mempunyai dampak negatif terhadap ekonomi dan pribadi.

Hak atas privasi adalah kemampuan individu untuk memutuskan siapa yang mempunyai informasi tentang dirinya dan bagaimana informasi tersebut digunakan. Konsep perlindungan data berarti bahwa individu mempunyai hak untuk memutuskan apakah akan membagikan atau menukar informasi pribadinya. Selain itu, individu juga berhak menentukan ketentuan transfer data pribadinya. Lebih lanjut, perlindungan data juga terkait dengan konsep hak privasi. Hak atas privasi telah berkembang digunakan untuk merumuskan hak untuk melindungi data pribadi. Indonesia telah mengambil langkah maju dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Namun, berbagai insiden kebocoran data mengindikasikan masih lemahnya kesiapan institusi pemerintah dalam memenuhi kewajiban tersebut. Oleh karena itu, sosialisasi mengenai kesadaran keamanan siber dan perlindungan data pribadi menjadi hal yang sangat fundamental untuk diimplementasikan kepada masyarakat dari kalangan manapun.

Sehubungan dengan hal tersebut Masyarakat di wilayah ini memiliki beragam karakteristik usia, tingkat ekonomi, dan pendidikan, namun umumnya masih kurang memahami pentingnya keamanan siber dan perlindungan data pribadi. Lingkungan masyarakat Kelurahan Tanah Merah, yang dekat dengan Universitas Mulawarman, menghadirkan peluang bagi dosen dan mahasiswa untuk melakukan pengabdian masyarakat. Hal ini menjadi tantangan tersendiri dalam upaya meningkatkan kesadaran mereka akan risiko dan penipuan daring yang semakin canggih. Pengabdian masyarakat ini memberikan edukasi yang mendalam agar masyarakat lebih waspada terhadap penggunaan teknologi dan memahami risiko keamanan siber, terutama terkait data pribadi

---

\*) Correspondenting Author

mereka. Pengabdian masyarakat ini dirasakan sangat tepat karena kesadaran keamanan siber dan perlindungan data pribadi saat ini menjadi hal yang sangat krusial, akan tetapi seringkali masyarakat belum memahami pentingnya hal tersebut.

Tujuan utama dari kegiatan pengabdian masyarakat ini adalah untuk meningkatkan pemahaman dan keterampilan masyarakat Kelurahan Tanah Merah mengenai keamanan siber, dengan harapan mereka dapat melindungi diri dari berbagai ancaman digital. Program ini dirancang untuk membantu masyarakat memahami jenis-jenis ancaman siber yang umum terjadi, seperti *phishing*, *malware*, dan pencurian identitas. Selain itu, pelatihan ini juga bertujuan untuk memanfaatkan perangkat digital seperti HP dan laptop yang sudah dimiliki masyarakat sebagai media belajar untuk meningkatkan kesadaran akan pentingnya keamanan data. Dengan adanya pelatihan ini, diharapkan masyarakat dapat membangun kebiasaan aman dalam berinternet dan memiliki keterampilan yang cukup untuk melindungi diri dari potensi serangan siber di masa depan.

## 2. METODE

Metode pelaksanaan kegiatan pengabdian masyarakat “Edukasi Keamanan Cyber untuk Melindungi Masyarakat dari Ancaman Digital” ini terdiri dari beberapa tahapan yang dirancang untuk memberikan edukasi mendalam tentang keamanan digital. Proses ini melibatkan penyampaian materi melalui metode lisan, demonstrasi praktis, serta pendekatan interaktif yang bertujuan untuk meningkatkan pemahaman dan keterampilan peserta dalam menjaga keamanan digital. Kegiatan ini diadakan pada Minggu, 22 September 2024.

### A. Solusi

Untuk mencapai tujuan program edukasi ini, berikut solusi yang diterapkan dalam setiap tahapan kegiatan:

- 1) Penyampaian Lisan : Pada awal pembahasan tiap pokok materi, metode lisan digunakan untuk menjelaskan teori dasar keamanan siber dan langkah-langkah praktis melindungi diri dari ancaman digital. Dengan metode ini, peserta dapat mengajukan pertanyaan secara langsung sehingga terjadi interaksi yang membantu memperdalam pemahaman mereka tentang materi.
- 2) Demonstrasi Praktik : Metode demonstrasi dilaksanakan dengan memperlihatkan cara menggunakan fitur keamanan pada aplikasi penting, seperti mobile banking (*Mbanking*), dompet digital (*Dana*, *OVO*, *Gopay*), Media Sosial (*Whatsapp*, *Facebook*, *Instagram*) dan *e-money*. Peserta diajarkan teknik transaksi aman, pengaturan privasi, serta tips menghindari penipuan saat berbelanja online. Demonstrasi ini bertujuan untuk memastikan peserta menguasai langkah-langkah praktis dalam menjaga keamanan digital mereka.

### B. Pendekatan

Beberapa pendekatan dilakukan untuk memastikan keberhasilan program ini:

- 1) Partisipatif : Masyarakat dilibatkan sebagai penerima materi dan diberikan kesempatan untuk berdiskusi dan bertanya kepada pemateri. Pendekatan ini memungkinkan peserta terlibat secara aktif dalam kegiatan, sehingga pengetahuan yang disampaikan dapat lebih mudah dipahami.
- 2) Kolaboratif : Program ini dilaksanakan dengan bekerja sama antara tim pengabdian masyarakat, dosen pembimbing, serta perwakilan masyarakat setempat. Kolaborasi ini membantu memperkuat hubungan dengan masyarakat dan memberikan dukungan dalam kelancaran acara.

### C. Prosedur Kerja

Tahapan pelaksanaan kegiatan ini adalah sebagai berikut:

- 1) Identifikasi Masalah : Tim melakukan observasi dan pengkajian masalah terkait kebutuhan edukasi keamanan digital di masyarakat, khususnya dalam pemanfaatan aplikasi keuangan dan media sosial yang aman.
- 2) Penentuan Tujuan : Berdasarkan identifikasi masalah, disusun tujuan program untuk memberikan edukasi menyeluruh mengenai keamanan siber.
- 3) Identifikasi Peserta : Sasaran peserta adalah masyarakat umum, khususnya yang belum memahami keamanan siber dalam penggunaan aplikasi keuangan dan media sosial.
- 4) Penjadwalan : Program dijadwalkan pada Minggu, 22 September 2024, dengan susunan acara yang terstruktur agar setiap materi dapat disampaikan dengan jelas.
- 5) Persiapan Materi dan Pemateri : Materi tentang keamanan digital dan cara penggunaannya disiapkan dengan lengkap. Pemateri dipilih dari ahli keamanan siber yang berpengalaman.
- 6) Penyediaan Fasilitas : Fasilitas pendukung seperti tempat pelatihan, alat presentasi, dan peralatan praktikum disiapkan untuk mendukung kelancaran acara.
- 7) Pengiriman Undangan : Undangan disebarluaskan kepada masyarakat sasaran melalui media sosial dan pengumuman langsung kepada masyarakat setempat.
- 8) Pelaksanaan : Kegiatan edukasi dilaksanakan sesuai susunan acara yang telah direncanakan. Peserta mengikuti penyampaian materi, sesi tanya jawab, serta demonstrasi praktis dengan arahan langsung dari tim pengabdian.
- 9) Dokumentasi : Seluruh rangkaian acara didokumentasikan untuk keperluan laporan kegiatan dan sebagai referensi untuk kegiatan mendatang.

10) Evaluasi : Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur pemahaman peserta. Dari evaluasi ini, tim pengabdian dapat mengevaluasi efektivitas program dan menyusun perbaikan untuk kegiatan selanjutnya.

#### **D. Pelaksanaan Kegiatan**

Kegiatan edukasi ini dilaksanakan pada hari Minggu, 22 September 2024, mulai pukul 09.00 hingga 16.00. Berikut adalah rincian pelaksanaannya:

- 1) Pembukaan (09.00 – 09.05)  
Acara dimulai dengan pembukaan oleh MC.
- 2) Pembacaan Doa (09.05 – 09.10)  
Dilakukan secara kondisional untuk mengawali acara dengan baik.
- 3) Sambutan (09.10 – 09.30)  
Sambutan diberikan oleh Ketua Pengabdian Masyarakat, Dosen Pembimbing, dan Ketua RT 22.
- 4) Pre-test (09.30 – 09.40)  
Peserta mengerjakan pre-test yang disiapkan oleh PJ tim untuk mengetahui pemahaman awal tentang keamanan siber.
- 5) Penyampaian Materi (09.40 – 11.00)  
Materi tentang keamanan siber disampaikan oleh pemateri, termasuk langkah-langkah menjaga keamanan di dunia digital.
- 6) Sesi Tanya Jawab (11.00 – 11.30)  
Peserta diberikan kesempatan bertanya untuk memperdalam pemahaman mereka.
- 7) Praktik (11.30 – 12.00, dilanjutkan setelah ISHOMA)  
Peserta mengikuti praktik tentang penggunaan aman aplikasi digital.
- 8) ISHOMA (12.00 – 13.00)  
Istirahat, Sholat, dan Makan.
- 9) Lanjutan Praktik (13.00 – 14.30)  
Peserta melanjutkan praktik menggunakan aplikasi digital dengan bimbingan tim.
- 10) Sesi Kuis dan Pemberian Hadiah (14.30 – 15.00)  
Kuis diberikan untuk menguji pemahaman peserta, dengan hadiah bagi yang berhasil menjawab dengan baik.
- 11) Penyerahan Plakat (15.00 – 15.05)  
Plakat diserahkan sebagai simbol apresiasi kepada peserta.
- 12) Post-test (15.05 – 15.30)  
Peserta mengerjakan post-test untuk mengevaluasi pemahaman yang diperoleh dari program.
- 13) Dokumentasi dan Penutup (15.30 – 16.00)  
Dokumentasi diambil, dan acara ditutup oleh MC.

### **3. HASIL DAN PEMBAHASAN**

Berdasarkan hasil kajian dan perencanaan yang telah dilakukan sebelumnya, kegiatan pengabdian masyarakat untuk meningkatkan pemahaman tentang keamanan siber di Kelurahan Tanah Merah dilaksanakan dengan pendekatan partisipatif dan kolaboratif. Kegiatan ini bertujuan untuk membangun kesadaran masyarakat terkait pentingnya melindungi data pribadi di era digital, terutama mengingat tingginya angka insiden kebocoran data yang terjadi di Indonesia. Menurut laporan Surfshark, lebih dari 97 juta akun di Indonesia telah menjadi korban kebocoran data sepanjang tahun 2020-2024, menempatkan Indonesia pada peringkat ke-8 secara global (Aristyo, 2024). Program ini melibatkan dosen dan mahasiswa Universitas Mulawarman sebagai fasilitator, serta dukungan masyarakat lokal. Tujuan utama kegiatan ini adalah untuk membantu masyarakat agar lebih waspada terhadap ancaman siber seperti phishing, malware, dan pencurian identitas, serta memberikan keterampilan praktis dalam menggunakan perangkat digital secara aman.

#### **A. Pelaksanaan Kegiatan**

Kegiatan edukasi keamanan siber dilaksanakan dengan tiga sesi utama, yakni sesi penyampaian materi, sesi praktik, dan sesi tanya jawab. Berikut adalah rincian pelaksanaan masing-masing sesi:

- 1) Penyampaian Materi Keamanan Cyber  
Sesi Penyampaian materi keamanan cyber dilakukan setelah acara pembukaan oleh dosen pembimbing pada Gambar 1 dan pretest oleh peserta pada Gambar 2. Acara pengabdian masyarakat yang dilakukan berfokus pada pemberian informasi dasar mengenai keamanan siber pada Gambar 3, termasuk berbagai jenis ancaman siber yang dapat dihadapi, seperti phishing, malware, dan pencurian identitas. Materi yang disampaikan juga mencakup tips praktis dalam melindungi data pribadi dan mengamankan perangkat digital. Pemateri dalam sesi ini adalah dosen dari Universitas Mulawarman yang memiliki latar belakang di bidang keamanan siber.



Gambar 1. Pembukaan Acara Oleh Dosen Pembimbing



Gambar 2. Pengerjaan *Pre-Test* Oleh Peserta



Gambar 3. Penyampaian Materi Oleh Pemateri

## 2) Praktik Implementasi Keamanan Cyber

Setelah sesi penyampaian materi, peserta diajak untuk langsung mempraktikkan cara-cara melindungi data pribadi mereka pada Gambar 4 dan dilanjutkan dengan mengerjakan posttest pada Gambar 5 untuk mengetahui seberapa paham peserta memahami materi yang disampaikan. Dalam sesi ini, peserta dibimbing untuk memahami langkah-langkah teknis yang dapat mereka lakukan secara mandiri guna meningkatkan keamanan data mereka. Melalui praktik langsung, peserta tidak hanya mendapatkan teori, tetapi juga pengalaman konkret yang dapat mereka aplikasikan dalam kehidupan sehari-hari, sehingga lebih memahami pentingnya proteksi data pribadi. Dengan bimbingan dari instruktur, peserta diajarkan cara mengenali tanda-tanda ancaman digital seperti email phishing atau situs web yang mencurigakan, serta cara menjaga keutuhan password agar tidak mudah diakses oleh pihak yang tidak berwenang. Selain itu, sesi ini juga menekankan pentingnya penggunaan perangkat lunak keamanan seperti antivirus dan pembaruan sistem untuk meminimalkan risiko kebocoran data. Praktik ini diharapkan dapat memberikan pemahaman yang lebih mendalam, membangun rasa percaya diri peserta, dan meningkatkan keterampilan mereka dalam mengelola data secara aman. Dengan demikian, peserta diharapkan dapat mengadopsi kebiasaan yang lebih aman dalam dunia digital, sekaligus turut berperan dalam menciptakan lingkungan online yang lebih terlindungi bagi diri mereka dan orang lain.



Gambar 4. Sesi Praktik Keamanan Akun



Gambar 5. Pengerjaan *Post-Test*

### 3) Tanya Jawab

Pada akhir kegiatan, sesi tanya jawab pada Gambar 6 dilakukan untuk memberikan kesempatan kepada peserta bertanya lebih lanjut mengenai materi yang disampaikan atau berbagi pengalaman terkait masalah keamanan siber yang pernah mereka alami. Sesi ini berlangsung interaktif dengan peserta yang antusias menanyakan berbagai topik seputar ancaman keamanan siber di lingkungan mereka. Fasilitator memberikan solusi-solusi yang relevan dan aplikatif sesuai dengan konteks lokal.



Gambar 6. Sesi Tanya Jawab

## B. Hasil Kegiatan

Berdasarkan evaluasi post-test, terdapat peningkatan pemahaman masyarakat tentang konsep dasar keamanan siber. Sebelum kegiatan, mayoritas peserta belum memahami cara melindungi akun media sosial atau dompet digital mereka. Namun, setelah kegiatan, peserta mampu mengidentifikasi langkah-langkah keamanan dasar. Masyarakat yang mengikuti sesi praktik menunjukkan kemampuan dalam menggunakan fitur keamanan di aplikasi digital. Mereka belajar cara mengatur privasi akun, mengaktifkan autentikasi dua faktor, dan mengenali tanda-tanda *phishing* (Putri, A., Sari, N., et al., 2025). Hasil dari sesi ini diukur dengan tes praktis yang menunjukkan peningkatan keterampilan peserta. Melalui sesi tanya jawab dan kuis, ditemukan peningkatan kesadaran peserta terhadap bahaya *phishing*, *malware*, dan pencurian identitas. Hal ini menunjukkan bahwa peserta tidak hanya memahami konsep, tetapi juga mengaplikasikan langkah-langkah perlindungan secara nyata.

## C. Dampak Kegiatan

Dengan meningkatnya pemahaman tentang pentingnya perlindungan data pribadi, masyarakat menjadi lebih berhati-hati dalam berinteraksi di dunia digital. Mereka lebih waspada terhadap risiko penggunaan aplikasi digital tanpa pengaturan keamanan yang tepat. Setelah mengikuti program ini, masyarakat menunjukkan perubahan perilaku dalam penggunaan teknologi. Mereka lebih sering menerapkan langkah-langkah keamanan yang telah diajarkan, seperti tidak sembarangan membagikan informasi pribadi dan mengaktifkan autentikasi dua faktor di akun-akun penting. Program ini berhasil menciptakan kesadaran di kalangan masyarakat bahwa mereka memiliki hak untuk melindungi data pribadi mereka. Dengan pemahaman ini, masyarakat menjadi lebih mandiri dan mampu melindungi diri dari ancaman digital.

## D. Implikasi dan Tindak Lanjut

Kegiatan pengabdian masyarakat ini memiliki potensi untuk ditindaklanjuti dengan program lanjutan, seperti pelatihan rutin atau pembentukan kelompok keamanan siber lokal yang dapat terus mengedukasi masyarakat sekitar tentang keamanan siber (Komansilan, T. et al., 2024). Dukungan berkelanjutan dari pihak universitas akan sangat membantu dalam memastikan dampak positif kegiatan ini tetap berlanjut.

- 1) Edukasi Berkelanjutan : Menyusun pelatihan keamanan siber yang diadakan secara berkala untuk memastikan masyarakat tetap update dengan ancaman keamanan siber terbaru.
- 2) *Local Leader* Keamanan Siber : Mendorong beberapa peserta yang antusias untuk menjadi pemimpin lokal yang akan membantu menjaga kesadaran keamanan siber di Kelurahan Tanah Merah. Local leader ini dapat berperan sebagai pendamping atau penyebar informasi ke warga lainnya.

## 4. KESIMPULAN

Kegiatan pengabdian masyarakat di Kelurahan Tanah Merah telah berhasil meningkatkan kesadaran dan pemahaman masyarakat mengenai pentingnya keamanan siber dan perlindungan data pribadi. Hasil kegiatan ini menunjukkan bahwa mayoritas peserta kini memahami risiko yang ada dalam dunia digital dan telah mengadopsi langkah-langkah dasar untuk melindungi data pribadi mereka, seperti mengaktifkan autentikasi dua faktor dan mengenali tanda-tanda *phishing* maupun *malware*. Partisipasi aktif dalam praktik dan sesi diskusi menegaskan bahwa metode yang diterapkan relevan dan efektif bagi masyarakat setempat.

Dampak signifikan lainnya adalah perubahan perilaku dalam penggunaan aplikasi digital secara aman, menunjukkan keberhasilan edukasi ini dalam meningkatkan kesadaran masyarakat terhadap ancaman digital. Keberhasilan kegiatan ini menunjukkan perlunya keberlanjutan program dengan mengadakan pelatihan berkala dan membentuk kelompok pemimpin keamanan siber lokal. Hal ini akan memastikan bahwa pengetahuan yang telah disampaikan terus diterapkan dan disebarluaskan, sehingga Masyarakat di Kelurahan Tanah Merah Samarinda dapat lebih mandiri dalam menjaga keamanan digital mereka.

## 5. PENGAKUAN/ UCAPAN TERIMA KASIH

Terima kasih yang sebesar-besarnya kepada semua pihak yang telah berperan dan membantu kegiatan serta kepada Lurah Tanah Merah beserta jajarannya yang telah memberikan dukungan dan fasilitas yang diperlukan. Ucapan terima kasih juga disampaikan kepada masyarakat Kelurahan Tanah Merah dan Ketua RT 22 yang telah menyambut baik kehadiran tim pengabdian dan berpartisipasi dalam kegiatan yang dilaksanakan.

## 6. DAFTAR PUSTAKA

- Akbar, A. (2024). *Peretasan, Kebocoran Data di Indonesia Terjadi Terus Menerus*. Retrieved from [tirto.id: https://tirto.id/melihat-jejak-kasus-peretasan-dan-kebocoran-data-di-indonesia-gUv1](https://tirto.id/melihat-jejak-kasus-peretasan-dan-kebocoran-data-di-indonesia-gUv1).
- Arham, M. R. H., & Risal, M. C. (2023). Perlindungan data pribadi bagi pengguna media sosial. *JURNAL AL TASYRI'IYYAH*, 109-119.

- Aristyo, R. (2024). *Indonesia jadi negara dengan tingkat kebocoran data terbesar*. Retrieved from Mashable Indonesia: <https://id.mashable.com/tech/2266/indonesia-jadi-negara-dengan-tingkat-kebocoran-data-terbesar>.
- Komansilan, T., Soesanto, E., & Salsabillah, N. (2024). Implementasi Keamanan Cyber Berbasis Nilai Nilai Kebangsaan UUD 1945 di Era Digital Best Practice di Perusahaan Pertamina. *Saturnus : Jurnal Teknologi Dan Sistem Informasi*, 2(3), 1–15.
- Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38-52. <https://doi.org/10.35870/jpni.v6i1.1097>.
- Septiani, L. (2023). *BSSN Catat Ada 207 Pencurian Data, Pemerintah Paling Banyak*. Retrieved from KataData: <https://katadata.co.id/digital/teknologi/6537ae3a29314/bssn-catat-ada-207-pencurian-data-pemerintah-paling-banyak>
- Setiawan, D. (2023). *Daftar Kasus Kebocoran Data di Indonesia Sepanjang 2023*. Retrieved from Viva: <https://www.viva.co.id/digital/digilife/1669505-daftar-kasus-kebocoran-data-di-indonesia-sepanjang-2023>.
- Wibawa, S., Suryanto, S., & Ningsih, R. (2024). Perlindungan Data Digital Dengan Time-Based One-Time Password (TOTP). *INSANtek*, 5(1), 30-36. <https://doi.org/10.31294/insantek.v5i1.3495>.
- Widianto, S., & A. T. (2024). *Cyber attack compromised Indonesia data centre, ransom sought*. Retrieved from Reuters: <https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/>
- Wulansari, E. M. (2020). Kosep Perlindungan Data Pribadi Sebagai Aspek. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan*, 265-289.