



Edukasi Keamanan Data dan Mitigasi Cybercrime bagi Masyarakat Pekon Kutawaringin Pringsewu

Sonianto^{1,*}, Fely Dany Prasetya¹, Ika Nuryana¹

¹Universitas Muhammadiyah Pringsewu, Lampung, Indonesia

Informasi Artikel

Sejarah Artikel:
Submit: 12 April 2026
Revisi: 22 April 2026
Diterima: 08 Mei 2026
Diterbitkan: 30 Mei 2026

Kata Kunci

Cybercrime, Keamanan Data, Literasi Digital

Correspondence

E-mail: sonianto@umpri.ac.id *

A B S T R A K

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran masyarakat Pekon Kutawaringin, Pringsewu, mengenai ancaman cybercrime dan pentingnya keamanan data pribadi. Kegiatan dilaksanakan melalui sosialisasi yang mencakup pemaparan jenis-jenis cybercrime, seperti phishing, malware, dan cyberstalking, serta langkah-langkah preventif untuk melindungi data pribadi di lingkungan digital. Peserta juga diberikan pelatihan mengenai penerapan kata sandi yang kuat, autentikasi dua faktor, dan pengelolaan privasi media sosial. Evaluasi kegiatan dilakukan melalui kuesioner sebelum dan sesudah pelatihan, yang menunjukkan adanya peningkatan rata-rata pemahaman peserta dari 20% menjadi 75%, atau meningkat sebesar 55 poin persentase. Hasil tersebut menunjukkan bahwa kegiatan edukasi yang dilaksanakan efektif dalam meningkatkan literasi digital dan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi. Dengan demikian, kegiatan ini berpotensi menjadi model intervensi edukatif yang relevan dalam upaya pencegahan risiko cybercrime di masyarakat.

Abstract

This community service program aimed to raise public awareness in Pekon Kutawaringin, Pringsewu, about cybercrime threats and the importance of personal data security. The program was delivered through educational sessions covering common forms of cybercrime, including phishing, malware, and cyberstalking, along with practical strategies for protecting personal data in digital settings. Participants were also trained to use strong passwords, enable two-factor authentication, and manage social media privacy more effectively. Evaluation findings based on pre- and post-training questionnaires showed an average improvement in participants' understanding from 20% to 75%, representing an increase of 55 percentage points. These results indicate that the program was effective in enhancing digital literacy and awareness of personal data protection. The activity also suggests that community-based education can serve as an effective approach to cybercrime prevention.

This is an open access article under the CC-BY-SA license



1. Pendahuluan

Seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, masyarakat semakin bergantung pada penggunaan internet untuk berbagai aktivitas, mulai dari komunikasi, transaksi, hingga pengolahan data pribadi. Namun, di balik kemudahan tersebut, muncul pula tantangan besar berupa ancaman terhadap keamanan siber, yang sering kali disebut sebagai cybercrime.

Cybercrime merujuk pada kejahatan yang dilakukan melalui jaringan internet yang dapat merugikan individu maupun organisasi. Jenis kejahatan ini meliputi peretasan, pencurian data

pribadi, penipuan online, penyebaran virus komputer, serta bentuk-bentuk kejahatan lain yang menargetkan pengguna internet[1]. Cybercrime dapat berdampak luas pada berbagai aspek kehidupan, termasuk ekonomi, politik, dan kehidupan pribadi[2]. Dampak tersebut semakin meluas seiring dengan meningkatnya adopsi teknologi digital oleh masyarakat[3].

Di Indonesia, kejahatan siber telah menjadi ancaman yang nyata dan semakin marak, seiring dengan peningkatan jumlah pengguna internet yang sangat pesat. Berdasarkan data dari Asosiasi Penyedia Jasa Internet Indonesia (APJII), jumlah pengguna internet Indonesia pada tahun 2023 telah mencapai lebih dari 200 juta orang, dengan sebagian besar pengguna mengakses internet melalui perangkat mobile [4]. Meskipun tingkat penetrasi internet semakin tinggi, pengetahuan masyarakat tentang risiko cybercrime dan pentingnya perlindungan data pribadi masih sangat terbatas [5].

Tingkat pemahaman yang rendah mengenai ancaman siber di tingkat masyarakat menjadi perhatian utama. Studi oleh [5] menunjukkan bahwa sebagian besar masyarakat Indonesia masih rentan terhadap serangan dunia maya, yang disebabkan oleh ketidaktahuan mereka tentang langkah-langkah preventif yang dapat diambil untuk menghindari ancaman tersebut, seperti penggunaan kata sandi yang kuat, enkripsi data, dan menjaga privasi informasi pribadi [6]. Sebagai akibatnya, banyak orang yang menjadi korban penipuan online, peretasan akun media sosial, dan pencurian data pribadi, yang berdampak pada kerugian finansial dan kepercayaan diri yang hilang.

Desa atau pekon, seperti Pekon Kutawaringin di Kabupaten Pringsewu, merupakan salah satu wilayah yang menunjukkan tantangan besar terkait pengetahuan mengenai cybercrime dan keamanan data pribadi. Di daerah ini, meskipun banyak warga yang mulai menggunakan internet dalam kehidupan sehari-hari, pemahaman tentang bagaimana cara melindungi data pribadi mereka dan mengidentifikasi potensi ancaman siber masih sangat terbatas. Sering kali, masyarakat setempat kurang mendapatkan pendidikan yang memadai mengenai pentingnya keamanan data pribadi, yang membuat mereka semakin rentan terhadap kejahatan siber yang kian canggih dan merugikan [7].

Selain itu, dengan semakin meningkatnya penggunaan media sosial dan platform digital lainnya, ancaman terhadap data pribadi semakin besar. Menurut [6], media sosial telah menjadi salah satu saluran utama bagi penjahat siber untuk mengakses data pribadi pengguna, yang terkadang tidak sadar dibagikan dengan mudah melalui platform digital ini [8].

Berdasarkan observasi awal dan hasil komunikasi singkat dengan perangkat Pekon Kutawaringin, ditemukan bahwa sebagian warga pernah mengalami atau mengetahui kasus penipuan melalui pesan digital, percobaan pengambilalihan akun media sosial, serta permintaan data pribadi dengan kedok tertentu. Perangkat pekon juga menyampaikan bahwa masih ada warga yang belum terbiasa menggunakan kata sandi yang kuat dan autentikasi dua faktor. Kondisi ini menunjukkan bahwa pemahaman masyarakat terhadap keamanan data pribadi masih perlu ditingkatkan melalui kegiatan edukasi yang terarah.

Pengabdian kepada masyarakat yang dilaksanakan ini bertujuan untuk mengatasi ketidakpahaman dan meningkatkan kesadaran masyarakat Pekon Kutawaringin, Pringsewu mengenai ancaman cybercrime dan keamanan data pribadi. Sejalan dengan hasil studi oleh [2], yang menekankan pentingnya sosialisasi yang menyeluruh dan berbasis pada literasi digital untuk meminimalisir dampak dari serangan dunia maya, kegiatan ini bertujuan untuk memberikan pemahaman yang lebih baik kepada masyarakat tentang ancaman-ancaman tersebut serta cara-cara melindungi diri mereka di dunia digital [9].

Keamanan data pribadi tidak hanya mencakup perlindungan terhadap data finansial, tetapi juga meliputi data pribadi yang lebih sensitif, seperti identitas dan riwayat kesehatan. Dalam konteks ini, penting bagi masyarakat untuk mengenal prinsip-prinsip dasar enkripsi dan penggunaan perangkat yang aman. Seperti yang dijelaskan oleh [8], salah satu cara utama untuk melindungi data pribadi adalah dengan menggunakan teknik enkripsi, yang dapat membantu mengamankan informasi

pribadi dari pihak yang tidak berwenang [10]. Dalam kegiatan ini, sosialisasi akan difokuskan pada pentingnya enkripsi, penggunaan kata sandi yang kuat, serta kewaspadaan terhadap aplikasi atau situs web yang berpotensi berbahaya.

Tujuan utama dari pengabdian ini adalah untuk meningkatkan kesadaran masyarakat Pekon Kutawaringin mengenai pentingnya perlindungan data pribadi dan ancaman cybercrime. Melalui pelatihan dan sosialisasi yang disesuaikan dengan kebutuhan lokal, masyarakat diharapkan dapat mengidentifikasi potensi ancaman dan mengadopsi langkah-langkah preventif yang efektif untuk melindungi data pribadi mereka dari serangan dunia maya. Sebagai tambahan, kegiatan ini juga bertujuan untuk membangun pemahaman yang lebih luas mengenai pentingnya keamanan data pribadi dalam kehidupan sehari-hari, serta dampak yang dapat ditimbulkan dari kelalaian dalam menjaga privasi di dunia digital.

2. Metode Pelaksanaan

2.1. Lokasi dan Waktu Pelaksanaan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di Pekon Kutawaringin Kecamatan Adiluwih, Kabupaten Pringsewu, Provinsi Lampung. Pemilihan lokasi ini dipilih karena meskipun penggunaan teknologi digital semakin berkembang di kalangan masyarakat, pemahaman tentang potensi ancaman cybercrime dan pentingnya keamanan data pribadi masih sangat terbatas. Oleh karena itu, penting untuk memberikan sosialisasi dan edukasi kepada masyarakat setempat mengenai cara-cara melindungi data pribadi mereka dari potensi serangan dunia maya, sebagaimana yang dijelaskan oleh [10] yang menyatakan bahwa perlindungan data menjadi kunci penting untuk menjaga keamanan individu dalam dunia digital.

Kegiatan ini dilaksanakan pada tanggal 28 Januari 2026, dengan durasi sesi pelatihan 4 jam. Waktu pelaksanaan dipilih pada pagi hari agar tidak mengganggu aktivitas utama peserta, yang sebagian besar bekerja di sektor informal seperti pertanian dan perdagangan. Pemilihan waktu ini juga mempertimbangkan kenyamanan peserta, agar mereka dapat mengikuti seluruh rangkaian pelatihan dengan baik dan penuh perhatian, sejalan dengan penjelasan oleh [11] yang menekankan pentingnya pemilihan waktu yang tepat untuk pelatihan yang dapat meningkatkan efektivitas pengajaran.

2.2. Kelompok Sasaran

Kelompok sasaran dalam kegiatan ini adalah warga Pekon Kutawaringin yang berusia 18 hingga 50 tahun. Kelompok ini dipilih berdasarkan fakta bahwa mereka lebih sering menggunakan perangkat digital untuk berbagai kebutuhan, baik itu untuk komunikasi, transaksi online, maupun aktivitas digital lainnya. Namun, pemahaman mereka mengenai risiko yang dapat timbul dari penggunaan teknologi masih terbatas mengingat masyarakat yang aktif dalam penggunaan teknologi namun minim pengetahuan tentang cybercrime rentan menjadi korban kejahatan siber [9].

Sebanyak 30 peserta dari berbagai latar belakang profesi, seperti petani, pedagang, aparatur pemerintah pekon, pemuda karang taruna, dan pekerja sektor informal lainnya, mengikuti kegiatan ini. Mereka dipilih untuk diberi pelatihan yang relevan dengan tantangan yang mereka hadapi sehari-hari, mengingat mereka memiliki potensi besar untuk mengadopsi pengetahuan dan keterampilan yang dapat melindungi diri dari ancaman dunia maya, seperti yang ditekankan oleh [12] tentang pentingnya memberikan pelatihan berbasis kebutuhan lokal dalam menjaga keamanan digital masyarakat.

2.3. Teknik Pengumpulan Data

Data pada kegiatan ini dikumpulkan melalui wawancara, kuesioner, dan observasi. Wawancara dilakukan sebelum kegiatan dimulai kepada beberapa perangkat pekon dan perwakilan peserta untuk memperoleh gambaran awal mengenai pemahaman masyarakat terhadap cybercrime dan

keamanan data pribadi [2]. Observasi dilakukan selama kegiatan berlangsung untuk menilai partisipasi, respons, dan keterlibatan peserta dalam setiap sesi [10].

Instrumen kuesioner digunakan untuk mengukur perubahan pemahaman peserta sebelum dan sesudah pelatihan. Kuesioner terdiri atas 5 butir pertanyaan yang disusun dalam bentuk jawaban tertutup dengan kategori benar/salah dan pilihan respons sederhana terkait pemahaman peserta terhadap cybercrime, perlindungan data pribadi, identifikasi phishing, penggunaan autentikasi dua faktor, serta persepsi keamanan setelah mengikuti kegiatan. Skor diberikan untuk setiap jawaban yang sesuai, kemudian dihitung dalam bentuk persentase untuk mengetahui tingkat pemahaman peserta sebelum dan sesudah pelatihan [3].

Simulasi dalam kegiatan ini dilaksanakan secara langsung menggunakan gawai milik peserta dengan pendampingan fasilitator. Pada tahap simulasi, peserta diminta mempraktikkan langkah-langkah perlindungan data pribadi, seperti membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor, mengatur privasi akun media sosial, serta mengenali pesan atau tautan yang mencurigakan. Fasilitator juga memberikan contoh tampilan pesan phishing dan menjelaskan langkah aman yang perlu dilakukan jika peserta menerima pesan serupa. Dengan demikian, simulasi tidak hanya berfungsi sebagai praktik teknis, tetapi juga sebagai sarana untuk memperkuat pemahaman peserta terhadap ancaman siber dalam situasi nyata.

Alur kegiatan pengabdian ditampilkan pada Gambar 1 yang menunjukkan tahapan kegiatan mulai dari persiapan materi, sosialisasi, diskusi interaktif, simulasi, hingga evaluasi. Diagram alir ini disusun untuk menggambarkan urutan pelaksanaan kegiatan secara sistematis.



Gambar 1. Alur Kegiatan Pengabdian

2.4. Analisis Data

Data yang terkumpul dari wawancara, kuesioner, simulasi, dan observasi akan dianalisis secara kuantitatif dan kualitatif. Data dari kuesioner akan dianalisis untuk menghitung persentase perubahan pemahaman peserta mengenai cybercrime dan perlindungan data pribadi sebelum dan setelah pelatihan. Analisis kuantitatif ini akan memberikan gambaran mengenai sejauh mana pelatihan ini berhasil meningkatkan kesadaran masyarakat tentang pentingnya melindungi data pribadi mereka di dunia maya. Pendekatan kuantitatif ini juga mendukung temuan [13] yang menyatakan bahwa pengukuran yang jelas dan sistematis adalah kunci untuk menilai dampak sebuah program edukasi tentang keamanan data pribadi.

Analisis kualitatif dilakukan dengan mengevaluasi hasil wawancara dan observasi untuk menggali pemahaman peserta mengenai cara-cara melindungi data pribadi mereka. Metode ini juga digunakan untuk memahami tantangan yang dihadapi peserta dalam mengimplementasikan pengetahuan yang diperoleh. Analisis kualitatif sangat penting untuk menggali lebih dalam persepsi dan pengalaman peserta yang tidak dapat diungkapkan hanya dengan data kuantitatif [11].

2.5. Penyajian Data

Hasil analisis data akan disajikan dalam bentuk grafik yang menunjukkan perbandingan skor pemahaman peserta sebelum dan setelah pelatihan. Grafik ini akan memberikan gambaran yang jelas mengenai seberapa besar peningkatan pemahaman mereka tentang ancaman cybercrime dan langkah-langkah perlindungannya. Selain itu, hasil wawancara dan observasi akan disajikan dalam bentuk narasi, menggambarkan tanggapan peserta, serta tantangan atau hambatan yang mereka hadapi dalam mengimplementasikan langkah-langkah perlindungan yang telah diajarkan selama pelatihan.

2.6. Alat dan Bahan

Beberapa alat dan bahan yang digunakan dalam kegiatan ini meliputi proyektor dan layar presentasi, yang digunakan untuk menampilkan materi pelatihan secara visual agar lebih mudah dipahami oleh peserta. Laptop dan perangkat lunak presentasi (Microsoft PowerPoint) digunakan untuk menyusun materi, sementara brosur dan leaflet yang berisi informasi tentang langkah-langkah perlindungan data pribadi dibagikan kepada peserta sebagai referensi setelah pelatihan. Kuesioner digunakan untuk mengumpulkan data yang diperlukan untuk evaluasi kegiatan, dan alat tulis digunakan untuk mencatat hasil wawancara dan umpan balik dari peserta [14].

3. Hasil dan Pembahasan

Kegiatan Sosialisasi Cybercrime dan Keamanan Data di Pekon Kutawaringin telah dilaksanakan dengan tujuan untuk meningkatkan kesadaran masyarakat mengenai ancaman dunia maya dan pentingnya perlindungan data pribadi. Melalui sesi pemaparan materi, diskusi interaktif, serta simulasi langkah-langkah perlindungan data, kegiatan ini berhasil memberikan pemahaman yang lebih baik kepada peserta. Berikut adalah hasil dari kegiatan tersebut yang didukung oleh data kuantitatif dan kualitatif.

3.1. Pemaparan Materi dan Pengenalan Cybercrime

Pada tahap pemaparan materi, peserta memperoleh penjelasan mengenai pengertian cybercrime, jenis-jenis ancaman siber, serta dampaknya terhadap individu maupun masyarakat. Materi ini menjadi dasar penting karena sebagian peserta masih memandang ancaman siber sebagai risiko yang jauh dari kehidupan sehari-hari. Setelah diberikan contoh konkret, peserta lebih mudah mengaitkan materi dengan pengalaman mereka sendiri, terutama yang berkaitan dengan penipuan melalui pesan digital dan penyalahgunaan akun media sosial.

Secara umum, peningkatan pemahaman pada aspek pengenalan cybercrime relatif tinggi karena materi yang disampaikan bersifat umum, dekat dengan pengalaman peserta, dan mudah dipahami. Hal ini sejalan dengan karakteristik edukasi dasar literasi digital, yaitu memberikan pengetahuan awal yang langsung relevan dengan aktivitas digital masyarakat. Dengan demikian, materi pengenalan cybercrime berperan sebagai pintu masuk untuk mendorong peserta memahami ancaman yang lebih spesifik pada tahap berikutnya.



Gambar 2. Pemaparan materi tentang ancaman *cybercrime* dan keamanan data

3.2. Diskusi Interaktif: Mengenali dan Menghindari Ancaman Phishing

Selama sesi diskusi interaktif, peserta diberi kesempatan untuk mendalami lebih jauh mengenai ancaman phishing. Peserta diberitahukan tentang cara-cara untuk mengidentifikasi email phishing, yang sering kali terlihat sah namun berisi tautan yang mengarah ke situs palsu. Beberapa cara untuk mengenali phishing adalah dengan memeriksa alamat pengirim, mengecek URL yang terdapat pada email atau pesan, serta tidak mengklik tautan sembarangan.

Selain itu, materi ini juga membahas pentingnya menggunakan autentikasi dua faktor (2FA) untuk mengamankan akun online mereka. Sebagai contoh, peserta diajarkan untuk mengaktifkan 2FA pada akun media sosial mereka untuk menambah lapisan perlindungan terhadap data pribadi.

3.3. Simulasi Langkah Perlindungan Data Pribadi

Simulasi langsung pada gawai peserta memberikan kontribusi penting dalam meningkatkan keterampilan praktis peserta. Pada tahap ini, peserta tidak hanya menerima penjelasan teoretis, tetapi juga mempraktikkan pengamanan akun secara langsung. Cara ini membantu peserta memahami langkah-langkah perlindungan data secara lebih konkret karena mereka melihat dan mencoba sendiri menu pengaturan pada perangkat yang biasa digunakan.

Dibandingkan materi yang bersifat konseptual, simulasi teknis seperti pengaturan privasi dan pembuatan kata sandi kuat cenderung membutuhkan waktu lebih lama untuk dipahami. Hal ini karena peserta memiliki tingkat kemampuan digital yang beragam, sehingga proses adopsi tidak seragam. Simulasi yang dilakukan secara langsung pada gawai peserta menjadi keunggulan kegiatan ini karena lebih aplikatif dan mendorong keterampilan praktis, bukan hanya pengetahuan pasif.

3.4. Simulasi Langkah Perlindungan Data Pribadi

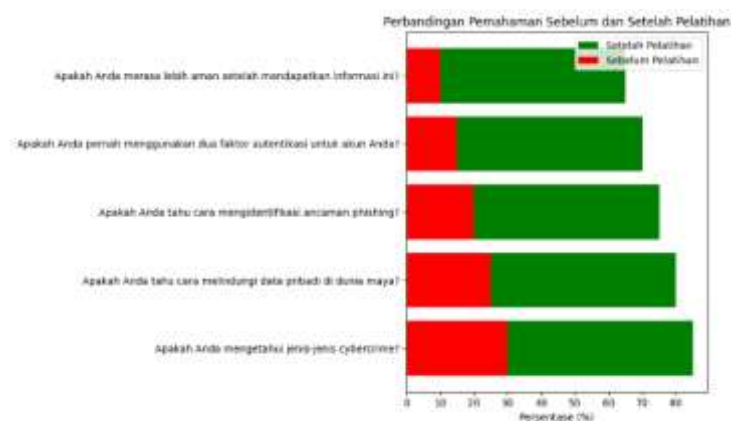
Untuk mengukur keberhasilan pelatihan, dilakukan pengukuran pemahaman peserta menggunakan kuesioner yang diberikan sebelum dan setelah kegiatan pelatihan. Tabel berikut menunjukkan perubahan persentase pemahaman peserta mengenai cybercrime dan keamanan data pribadi. Dari hasil pengukuran tersebut terlihat bahwa seluruh indikator mengalami peningkatan setelah peserta mengikuti kegiatan sosialisasi. Peningkatan paling tinggi terjadi pada pemahaman mengenai jenis-jenis cybercrime dan cara melindungi data pribadi di dunia maya, sedangkan peningkatan yang relatif lebih rendah terdapat pada penggunaan autentikasi dua faktor.

Perbedaan tingkat peningkatan ini menunjukkan bahwa materi yang bersifat konseptual dan dekat dengan pengalaman sehari-hari peserta, seperti pengenalan cybercrime dan phishing, lebih mudah dipahami dibandingkan materi yang memerlukan penerapan teknis secara langsung, seperti autentikasi dua faktor. Selain itu, evaluasi juga menunjukkan bahwa peserta masih menghadapi beberapa tantangan dalam menerapkan mitigasi kejahatan siber, antara lain keterbatasan pemahaman terhadap istilah teknis, kebiasaan menggunakan kata sandi yang sama pada beberapa akun, serta kurangnya kehati-hatian dalam membuka tautan atau pesan dari sumber yang tidak dikenal. Sebagian peserta juga menyampaikan bahwa mereka belum sepenuhnya percaya diri untuk mengatur fitur keamanan pada perangkat digital secara mandiri.

Temuan tersebut mengindikasikan bahwa peningkatan pemahaman peserta belum sepenuhnya diikuti oleh perubahan perilaku digital yang konsisten. Oleh karena itu, diperlukan pendampingan lanjutan dan pengulangan praktik secara berkala agar peserta dapat lebih terampil dalam menerapkan langkah-langkah mitigasi kejahatan siber dalam aktivitas sehari-hari.

Tabel 1. Presentase Pemahaman Peserta Sebelum dan Setelah Pemaparan Materi

Pertanyaan	Sebelum Pelatihan (%)	Setelah Pelatihan (%)
Apakah Anda mengetahui jenis-jenis <i>cybercrime</i> ?	30	85
Apakah Anda tahu cara melindungi data pribadi di dunia maya?	25	80
Apakah Anda tahu cara mengidentifikasi ancaman phishing?	20	75
Apakah Anda pernah menggunakan dua faktor autentikasi untuk akun Anda?	15	70
Apakah Anda merasa lebih aman setelah mendapatkan informasi ini?	10	65



Gambar 3. Grafik perbandingan pemahaman sebelum dan setelah pelatihan

Dari tabel dan grafik tersebut, dapat dilihat bahwa terdapat peningkatan yang signifikan dalam pemahaman peserta mengenai cybercrime dan keamanan data pribadi. Sebelum pelatihan, hanya sekitar 30% peserta yang mengetahui jenis-jenis cybercrime, sedangkan setelah pelatihan, angka tersebut meningkat hingga 85%. Hal serupa terjadi pada pertanyaan mengenai perlindungan data pribadi, di mana pemahaman peserta meningkat dari 25% menjadi 80%. Peningkatan signifikan juga terlihat pada pemahaman mengenai phishing dan penggunaan dua faktor autentikasi, yang sebelumnya hanya diketahui oleh 20% dan 15% peserta, kini meningkat menjadi 75% dan 70% setelah pelatihan.

3.5. Perbandingan dengan Penelitian Terdahulu

Jika dibandingkan dengan penelitian[11], tentang privasi dan keamanan data di media sosial, kegiatan ini memiliki kekhasan pada fokus penerapan langsung melalui simulasi di gawai peserta, bukan hanya penyampaian strategi pencegahan secara umum. Sementara itu, penelitian [12] menekankan peran strategis enkripsi dalam melindungi data di dunia digital, sedangkan pengabdian ini lebih menekankan penerapan praktis yang dekat dengan kebutuhan masyarakat awam, seperti pengenalan phishing, penguatan kata sandi, dan pengaturan privasi akun. Hal ini membuat pengabdian ini lebih kontekstual karena disesuaikan dengan kondisi sosial dan kemampuan digital masyarakat desa.

Selain itu, [13] menyoroti pentingnya perlindungan data pribadi di era digital secara umum, sedangkan kegiatan ini memperlihatkan implementasi langsung di tingkat komunitas melalui sosialisasi, diskusi, dan simulasi. Perbedaan utama kegiatan ini dengan penelitian sejenis terletak pada sasaran peserta, yaitu masyarakat pekon dengan latar belakang beragam, serta pada metode pembelajaran yang menekankan praktik langsung pada perangkat pribadi peserta. Dengan demikian, kontribusi kegiatan ini bukan hanya pada peningkatan pengetahuan, tetapi juga pada pembentukan kebiasaan aman dalam penggunaan teknologi sehari-hari.

3.6. Implikasi Kegiatan

Secara keseluruhan, hasil kegiatan menunjukkan bahwa edukasi keamanan data dan mitigasi cybercrime efektif dalam meningkatkan kesadaran digital masyarakat. Namun, hasil evaluasi juga menegaskan bahwa materi yang bersifat teknis, seperti autentikasi dua faktor, memerlukan pengulangan dan pendampingan lanjutan agar benar-benar diterapkan oleh peserta. Temuan ini penting karena menunjukkan bahwa keberhasilan pengabdian tidak hanya diukur dari peningkatan skor evaluasi, tetapi juga dari sejauh mana peserta mampu mengubah perilaku digital mereka.

Kegiatan ini menegaskan bahwa model pengabdian berbasis kebutuhan lokal, simulasi langsung, dan diskusi interaktif lebih efektif untuk masyarakat yang memiliki literasi digital beragam. Dengan

pendekatan tersebut, masyarakat tidak hanya memperoleh pengetahuan dasar, tetapi juga keterampilan praktis yang dapat digunakan untuk melindungi diri dari ancaman siber.

4. Kesimpulan

Kegiatan pengabdian kepada masyarakat yang bertemakan Sosialisasi Cybercrime dan Keamanan Data di Pekon Kutawaringin berhasil mencapai tujuan utamanya, yaitu meningkatkan kesadaran masyarakat tentang ancaman cybercrime dan pentingnya perlindungan data pribadi. Melalui pemaparan materi yang jelas, diskusi interaktif, dan simulasi langkah-langkah praktis, peserta menunjukkan peningkatan pemahaman yang signifikan mengenai berbagai jenis ancaman siber, seperti phishing, malware, dan cyberstalking, serta cara-cara efektif untuk melindungi data pribadi mereka, termasuk penggunaan kata sandi yang kuat, autentikasi dua faktor, dan pengaturan privasi yang lebih ketat. Hasil evaluasi menunjukkan bahwa lebih dari 50% peserta mengalami peningkatan pemahaman yang sangat besar mengenai pentingnya menjaga keamanan data pribadi mereka setelah mengikuti pelatihan ini. Peserta juga merasa lebih siap untuk menghadapi berbagai bentuk kejahatan dunia maya yang semakin berkembang.

Kegiatan ini tidak hanya memberikan pengetahuan dasar yang sangat diperlukan, tetapi juga menciptakan kesadaran baru di kalangan masyarakat mengenai betapa pentingnya keamanan data pribadi di dunia digital. Dengan adanya peningkatan yang cukup signifikan dalam pemahaman peserta, diharapkan masyarakat Pekon Kutawaringin dapat lebih waspada dan terlindungi dari ancaman siber yang semakin canggih.

Berdasarkan hasil pengabdian ini, disarankan agar kegiatan serupa dapat dilanjutkan secara berkala untuk memberikan pengetahuan yang lebih mendalam tentang topik-topik yang lebih teknis, seperti enkripsi data, keamanan perangkat keras, dan perangkat lunak pengaman. Mengingat bahwa ancaman cybercrime terus berkembang, penting untuk memastikan bahwa masyarakat terus memperoleh pembaruan terkait cara melindungi diri mereka di dunia digital. Selain itu, untuk memperluas dampak positif dari pengabdian ini, diharapkan dapat dilakukan pengabdian lanjutan yang melibatkan lebih banyak peserta dari berbagai lapisan masyarakat. Dengan adanya pelatihan berkelanjutan, diharapkan kesadaran akan keamanan data pribadi semakin menyebar, dan masyarakat dapat semakin memitigasi potensi ancaman dunia maya secara efektif.

Ucapan Terimakasih

Kami mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Muhammadiyah Pringsewu atas dukungan dan fasilitas yang diberikan, sehingga kegiatan pengabdian kepada masyarakat ini dapat terlaksana dengan baik. Terima kasih juga kami sampaikan kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) yang telah memberikan arahan, dukungan administratif, serta bimbingan yang sangat berharga dalam setiap tahap kegiatan ini. Tidak lupa, kami juga mengucapkan terima kasih kepada Pemerintah Pekon Kutawaringin yang telah mendukung penuh pelaksanaan sosialisasi ini dan memungkinkan kami untuk berbagi pengetahuan kepada masyarakat setempat. Tanpa dukungan dari pihak-pihak tersebut, kegiatan pengabdian ini tidak akan berjalan dengan sukses.

Daftar Pustaka

- [1] Marcum, C. D., & Higgins, G. E. (2019). *Cybercrime*. In *Handbook on crime and deviance* (pp. 459-475). Cham: Springer International Publishing.
- [2] Huber, E. (2019). *Cybercrime*. In *Cybercrime: Eine Einführung* (pp. 21-29). Wiesbaden: Springer Fachmedien Wiesbaden.
- [3] Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and society*.
- [4] Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Technology and Economics Law Journal*, 2(2), 3.

- [5] Chintia, E., Nadiyah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology* ISSN, 2549, 869X.
- [6] Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyashah*, 9(2), 118-13.
- [7] Sitanggang, A. S., Darmawan, F., & Saputra, D. (2024). Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber. *Jurnal Pendidikan Dan Teknologi Indonesia*, 4(3), 79-83.
- [8] Kehista, A. P., 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*, 4(5), 625-632.
- [9] Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145-160.
- [10] Gunawan, I. & Kom, M. (2021). *Keamanan data: Teori dan implementasi*. CV Jejak (Jejak Publisher).
- [11] Rahmawati, D., Aksana, M. D. A., & Mukaromah, S. (2023, November). Privasi dan keamanan data di media sosial: dampak negatif dan strategi pencegahan. In *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* (Vol. 3, No. 1, pp. 571-580).
- [12] Almadira, A., Pratama, Y., & Purwani, F. (2024). Melindungi Data Di Dunia Digital: Peran Strategis Enkripsi Dalam Keamanan Data. *Journal of Scientech Research and Development*, 6(2), 540-549.
- [13] Baqis, A. M., & Nasution, M. I. P. (2025). Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital. *Jurnal Manajemen Dan Pendidikan Agama Islam*, 3(3), 396-404.
- [14] Astuti, N. R. D. P., Natsir, F., Haris, M. S., Ramdhani, Y., Aribowo, E., Anwar, N., ... & Maniah, M. (2025). Keamanan Data dalam Revolusi Teknologi.