JURNAL PENGABDIAN MASYARAKAT MENTARI
e-ISSN : 3063 - 7066
Volume 3, No. 2, Tahun 2026
https://jurnalpengabdianmasyarakatmentari.com/index.php/jpmm/index

Edukasi Keamanan Digital Masyarakat melalui Pengenalan Hoaks, Perlindungan Data Pribadi, dan Pencegahan Phishing Bagi Karang Taruna RW 09 Kebon Bawang

Rosani Zalukhu[1], Gustri Dede Putra[2], Mohammad Jibril[3], Jonision A. Sigalingging[4], Teddy Septian Army[5], Refli Anggara[6], Fahmi Hakim[7], Naftika Umi Kulsum[8], Siti Choliza[9], Faurezi Samudra[10], Dwi Nurwiyanti[11], Indrawati[12]

[1,2,3,4,5,6,7,8,9,10,11,12] *Universitas 17 Agustus 1945 Jakarta, Indonesia*

Received : 3 September 2026, Revised : 10 September 2026, Published : 16 September 2026

Corresponding Author
Nama Penulis: Rosani Zalukhu
E-mail: rosanizalukhu23@gmail.com

Abstrak

Keamanan digital menjadi kebutuhan penting bagi masyarakat yang semakin aktif menggunakan telepon pintar, media sosial, dan berbagai layanan digital. Penggunaan teknologi yang tidak disertai pemahaman yang memadai dapat meningkatkan risiko terpapar hoaks, kebocoran data pribadi, serta phishing dan penipuan digital. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan pemahaman masyarakat dalam mengenali dan mencegah berbagai risiko keamanan digital tersebut. Kegiatan dilaksanakan pada 10 Agustus 2026 di Kebon Bawang, RW 09, Kecamatan Tanjung Priok, Jakarta Utara, dengan melibatkan 9 peserta dari masyarakat setempat. Metode kegiatan meliputi identifikasi kebutuhan, penyusunan materi, edukasi partisipatif, diskusi, pendampingan, simulasi kasus, monitoring, serta evaluasi melalui pre-test dan post-test. Instrumen evaluasi terdiri atas 11 pertanyaan tertutup dengan respons "Ya" dan "Tidak" yang mencakup pengenalan hoaks, perlindungan data pribadi, serta phishing dan penipuan digital. Materi disampaikan menggunakan presentasi dan leaflet dengan prinsip "Berhenti–Periksa–Bagikan", disertai simulasi pesan hadiah dengan tautan mencurigakan dan telepon yang meminta kode OTP. Hasil evaluasi menunjukkan bahwa persentase respons "Ya" meningkat dari 95,96% pada pre-test menjadi 100% pada post-tes, atau meningkat sebesar 4,04 poin persentase. Peningkatan terbesar terdapat pada indikator phishing dan penipuan digital, yaitu sebesar 11,11 poin persentase. Hasil tersebut menunjukkan adanya penguatan pemahaman peserta setelah mengikuti kegiatan edukasi. Evaluasi dilakukan segera setelah kegiatan sehingga belum dapat menggambarkan perubahan perilaku dan keterampilan peserta dalam jangka panjang. Pendekatan edukasi berbasis kasus dan simulasi dapat menjadi alternatif dalam penguatan pemahaman keamanan digital pada kelompok masyarakat dengan karakteristik penggunaan media digital yang serupa.

Kata kunci - *data pribadi, keamanan digital, literasi digital, phishing, hoaks*

Abstract

Digital security has become an important need for communities that are increasingly active in using smartphones, social media, and various digital services. The use of technology without adequate understanding may increase the risk of exposure to hoaxes, personal data breaches, phishing, and digital fraud. This community service activity aimed to improve participants' understanding of how to recognize and prevent various digital security risks. The activity was conducted on August 10, 2026, in Kebon Bawang, RW 09, Tanjung Priok District, North Jakarta, involving 9 local community participants. The activity consisted of needs identification, material preparation, participatory education, discussion, assistance, case simulations, monitoring, and evaluation through pre-test and

post-test. The evaluation instrument consisted of 11 closed-ended questions with "Yes" and "No" responses covering hoax recognition, personal data protection, and phishing and digital fraud. The materials were delivered through presentations and leaflets using the "Stop–Check–Share" principle, accompanied by simulations involving a prize message with a suspicious link and a phone call requesting an OTP code. The evaluation results showed that the percentage of "Yes" responses increased from 95.96% in the pre-test to 100% in the post-test, representing an increase of 4.04 percentage points. The largest increase was found in the phishing and digital fraud indicator, which increased by 11.11 percentage points. These results indicate an improvement in participants' understanding after the educational activity. However, the evaluation was conducted immediately after the activity and therefore could not reflect long-term changes in participants' behavior and skills. A case- and simulation-based educational approach can serve as an alternative for strengthening digital security understanding among community groups with similar patterns of digital technology use.
Keywords - *digital security, digital literacy, personal data, phishing, hoax*

How To Cite : *Zalukhu, R., Putra, G. D., Jibril, M., Sigalingging, J. A., Army, T. S., Anggara, R., … Indrawati, I. (2026). Edukasi Keamanan Digital Masyarakat melalui Pengenalan Hoaks, Perlindungan Data Pribadi, dan Pencegahan Phishing Bagi Karang Taruna RW 09 Kebon Bawang . Jurnal Pengabdian Masyarakat Mentari, 3(2), 300 - 313. https://doi.org/10.59837/jpmm.v3i2.408*

PENDAHULUAN

Perkembangan teknologi digital telah memberikan banyak kemudahan bagi masyarakat dalam menjalankan berbagai aktivitas sehari-hari (M.T et al., 2022). Smartphone saat ini tidak hanya digunakan sebagai alat komunikasi, tetapi juga menjadi sarana untuk melakukan transaksi perbankan, berbelanja secara daring, memperoleh informasi, menggunakan media sosial, serta mengakses berbagai layanan publik. Ketergantungan terhadap perangkat digital tersebut menjadikan keamanan informasi dan perlindungan data pribadi sebagai aspek yang semakin penting dalam kehidupan Masyarakat (Dijah Rahajoe et al., 2021).

Di balik kemudahan tersebut, masyarakat juga menghadapi berbagai risiko keamanan digital yang semakin beragam seiring dengan meningkatnya penggunaan teknologi dalam kehidupan sehari-hari (I. Purnama, 2020). Penggunaan telepon pintar dan internet membuat masyarakat lebih mudah menerima, menyimpan, dan membagikan informasi dalam waktu singkat. Kondisi ini memberikan banyak manfaat, tetapi di sisi lain juga dapat membuka peluang terjadinya berbagai ancaman apabila tidak diikuti dengan pengetahuan dan kewaspadaan yang memadai (Zalukhu et al., 2026). Salah satu ancaman yang sering ditemui adalah penyebaran informasi palsu atau hoaks. Informasi yang tidak benar dapat dikemas seolah-olah berasal dari sumber terpercaya sehingga masyarakat dapat mempercayainya tanpa melakukan pemeriksaan terlebih dahulu .

Ketika informasi tersebut langsung diteruskan kepada orang lain, penyebarannya dapat berlangsung dengan cepat dan menjangkau lebih banyak orang. Oleh karena itu, masyarakat perlu memiliki kemampuan untuk mengenali sumber informasi, memeriksa kebenaran isi, memperhatikan waktu dan konteks informasi, serta membandingkannya dengan sumber yang terpercaya. Dalam penelitian yang dilakukan oleh (Alpayed et al., 2025) menunjukkan bahwa literasi digital diperlukan untuk membantu masyarakat menghadapi penyebaran berita palsu, terutama dalam memilah dan memahami informasi sebelum mempercayai maupun menyebarkannya.

Selain hoaks, risiko keamanan digital juga berkaitan dengan perlindungan data pribadi. Dalam aktivitas sehari-hari, masyarakat sering memberikan berbagai informasi pribadi ketika membuat akun, menggunakan aplikasi, melakukan transaksi, mengakses layanan perbankan, maupun berkomunikasi melalui media sosial (Dijah Rahajoe et al., 2021). Data seperti nama lengkap, nomor identitas, alamat, nomor telepon, alamat surat elektronik, informasi rekening, kata sandi, PIN, dan kode *One-Time*

Password (OTP) merupakan informasi yang perlu dijaga karena dapat disalahgunakan apabila diketahui oleh pihak yang tidak bertanggung jawab (Dinihari et al., 2025). Kurangnya pemahaman mengenai perlindungan data pribadi dapat membuat seseorang memberikan informasi kepada pihak yang tidak dikenal, menggunakan kata sandi yang sama pada beberapa akun, atau memberikan akses aplikasi tanpa memperhatikan kebutuhan dan keamanannya (Illahi & Rita Gani, 2024). Kondisi tersebut dapat meningkatkan risiko penyalahgunaan identitas, pengambilalihan akun, hingga kerugian finansial. Dengan demikian, menjaga keamanan digital tidak hanya berkaitan dengan perangkat yang digunakan, tetapi juga dengan bagaimana seseorang mengelola dan melindungi informasi pribadinya (Istoningtyas et al., 2023).

Risiko lainnya adalah phishing, yaitu upaya penipuan dengan menyamar sebagai pihak yang dipercaya untuk memperoleh informasi rahasia seperti kata sandi, PIN, kode *One-Time Password* (OTP), atau informasi keuangan (Krisnawati et al., 2023). Pelaku dapat menggunakan identitas yang menyerupai bank, perusahaan, lembaga pemerintah, layanan pengiriman, maupun orang yang dikenal sehingga pesan yang diterima terlihat meyakinkan. Modus tersebut dapat dilakukan melalui pesan singkat, aplikasi komunikasi, surat elektronik, telepon, tautan palsu, maupun file atau aplikasi yang berasal dari sumber tidak dikenal. Dalam buku yang ditulis oleh (M.T et al., 2022) menunjukkan pentingnya pemahaman mengenai pengelolaan data pribadi dalam menghadapi berbagai risiko di ruang digital, termasuk ancaman yang memanfaatkan kelengahan pengguna untuk memperoleh informasi pribadi (H. Purnama et al., 2024). Dalam praktiknya, masyarakat dapat menerima pesan yang menggunakan bahasa mendesak, menawarkan hadiah, memberitahukan adanya masalah pada akun, atau meminta pengguna segera melakukan tindakan tertentu. Situasi tersebut dapat mendorong seseorang bertindak secara spontan tanpa terlebih dahulu memastikan kebenaran informasi atau identitas pihak yang menghubungi (Putri et al., 2025).

Berbagai bentuk ancaman tersebut memiliki pola yang hampir sama, yaitu memanfaatkan ketidaktelitian, ketergesaan, dan kurangnya kewaspadaan pengguna ketika menerima informasi atau permintaan di ruang digital (Putri Silmina et al., 2025). Seseorang dapat saja memahami bahwa hoaks, pencurian data, dan phishing merupakan ancaman, tetapi dalam situasi nyata masih dapat mengalami kesulitan ketika harus menentukan apakah suatu pesan, tautan, permintaan data, atau panggilan telepon dapat dipercaya. Kondisi ini menunjukkan bahwa pengetahuan mengenai keamanan digital perlu disertai dengan kemampuan untuk mengenali situasi yang mencurigakan dan menentukan tindakan yang tepat sebelum meresponsnya (Putri Silmina et al., 2025).

Perkembangan penggunaan teknologi digital juga perlu diikuti dengan peningkatan kemampuan masyarakat dalam menggunakannya secara aman. Berdasarkan hasil pengukuran Indeks Masyarakat Digital Indonesia (IMDI) tahun 2024, skor indeks masyarakat digital Indonesia mencapai 43,34, sedangkan pilar keterampilan digital berada pada angka 58,25 (Kominfo, 2025). Data tersebut menunjukkan bahwa peningkatan kompetensi digital masyarakat tetap perlu diikuti dengan penguatan kemampuan menggunakan teknologi secara aman dan bertanggung jawab termasuk dalam memahami dan menerapkan keamanan digital. Selain itu, Kementerian Komunikasi dan Digital mengidentifikasi 1.923 konten hoaks sepanjang tahun 2024, dengan kategori penipuan sebagai temuan terbanyak, yaitu sebanyak 890 konten. Kondisi tersebut menunjukkan bahwa kemampuan masyarakat dalam mengenali informasi yang meragukan dan menghadapi berbagai bentuk penipuan digital masih menjadi hal yang penting untuk diperhatikan (Kominfo, 2025).

Kondisi tersebut juga relevan dengan kegiatan pengabdian kepada masyarakat yang dilaksanakan bagi Karang Taruna RW 09 Kebon Bawang, Kecamatan Tanjung Priok, Jakarta Utara. Berdasarkan hasil observasi awal dan asesmen kebutuhan terhadap 9 peserta, diketahui bahwa peserta telah menggunakan smartphone dan berbagai layanan digital dalam aktivitas sehari-hari. Hasil pre-test menunjukkan bahwa dari 99 respons pada 11 pertanyaan, terdapat 95 respons "Ya" atau sebesar 95,96%, sedangkan 4 respons lainnya merupakan respons "Tidak". Hasil tersebut menunjukkan bahwa pemahaman awal peserta mengenai keamanan digital secara umum sudah relatif tinggi, tetapi masih

terdapat beberapa aspek yang membutuhkan penguatan, terutama pada pengenalan phishing dan penipuan digital serta pengenalan ciri-ciri informasi yang mencurigakan. Kondisi awal tersebut menunjukkan bahwa kebutuhan mitra tidak hanya berkaitan dengan pemberian informasi mengenai keamanan digital, tetapi juga penguatan pemahaman melalui contoh kasus dan simulasi yang dekat dengan penggunaan smartphone dan media digital sehari-hari (Siti Mutmainah et al., 2025).

Sejumlah penelitian dan kegiatan pengabdian kepada masyarakat menunjukkan bahwa edukasi literasi digital dapat membantu meningkatkan pemahaman masyarakat dalam menghadapi berbagai risiko di ruang digital (Utomo et al., 2024). Namun, kegiatan edukasi yang berfokus pada penyampaian materi belum selalu memberikan kesempatan kepada peserta untuk berlatih mengenali ancaman dalam situasi yang menyerupai penggunaan digital sehari-hari (Siti Mutmainah et al., 2025). Oleh karena itu, diperlukan pendekatan edukasi yang tidak hanya memberikan pengetahuan, tetapi juga melibatkan contoh kasus dan simulasi agar peserta dapat menghubungkan materi dengan situasi yang mungkin mereka hadapi (Wirajaya et al., 2024). Dalam konteks Karang Taruna RW 09 Kebon Bawang, pendekatan tersebut diterapkan dengan menggabungkan edukasi mengenai hoaks, perlindungan data pribadi, dan phishing dalam satu rangkaian kegiatan yang disertai metode "Berhenti–Periksa–Bagikan" serta simulasi kasus yang dekat dengan penggunaan smartphone sehari-hari. Pendekatan ini menjadi pembeda kegiatan karena peserta tidak hanya menerima informasi mengenai ancaman digital, tetapi juga memperoleh kesempatan untuk mengenali ciri-ciri ancaman dan menentukan respons yang tepat melalui situasi yang disimulasikan.

Berdasarkan permasalahan tersebut, kegiatan pengabdian kepada masyarakat melalui Kuliah Kerja Nyata Universitas 17 Agustus 1945 Jakarta dilaksanakan bagi Karang Taruna RW 09 Kebon Bawang dengan memberikan edukasi mengenai keamanan digital. Materi difokuskan pada tiga permasalahan yang berkaitan dengan aktivitas digital peserta, yaitu kemampuan mengenali hoaks, perlindungan data pribadi, serta kewaspadaan terhadap phishing dan penipuan digital. Kegiatan dilaksanakan melalui pemaparan materi, penerapan metode "Berhenti–Periksa–Bagikan" untuk membantu peserta menyaring informasi, serta simulasi kasus berupa pesan hadiah dan telepon yang meminta kode One-Time Password (OTP) (Zalukhu et al., 2026).

Pendekatan tersebut dipilih karena permasalahan keamanan digital tidak hanya berkaitan dengan pengetahuan mengenai jenis ancaman, tetapi juga kemampuan pengguna dalam mengambil keputusan ketika menghadapi situasi yang mencurigakan. Melalui contoh kasus dan simulasi, peserta dapat berlatih mengenali tanda-tanda ancaman serta menentukan respons yang tepat berdasarkan situasi yang menyerupai penggunaan digital sehari-hari (Rosihan & Novitasari, 2022). Dengan demikian, pendekatan berbasis kasus dan praktik diharapkan lebih sesuai dengan kebutuhan mitra dibandingkan edukasi yang hanya berfokus pada penyampaian informasi.

Kegiatan pengabdian ini bertujuan untuk meningkatkan pemahaman anggota Karang Taruna RW 09 Kebon Bawang mengenai keamanan digital, khususnya dalam mengenali hoaks, melindungi data pribadi, serta mengenali dan mencegah phishing dan penipuan digital. Secara praktis, kegiatan ini diarahkan agar peserta mampu mengenali tanda-tanda ancaman digital, menentukan tindakan yang tepat ketika menerima informasi atau permintaan yang mencurigakan, serta menerapkan perilaku digital yang lebih aman dalam penggunaan smartphone dan layanan digital sehari-hari. Selain itu, kegiatan ini diharapkan dapat menjadi salah satu bentuk edukasi keamanan digital berbasis kasus yang dapat diterapkan pada kelompok masyarakat dengan karakteristik penggunaan media digital yang serupa.

METODE

Kegiatan pengabdian kepada masyarakat dilaksanakan sebagai bagian dari program Kuliah Kerja Nyata (KKN) Universitas 17 Agustus 1945 Jakarta pada tanggal 10 Agustus 2026 di Kebon Bawang, RW 09, Kecamatan Tanjung Priok, Jakarta Utara. Peserta berjumlah 9 orang yang merupakan masyarakat setempat yang menggunakan smartphone dan aktif menggunakan media digital seperti

WhatsApp, media sosial, atau layanan digital lainnya. Kegiatan melibatkan tim KKN sebagai fasilitator dan masyarakat sebagai peserta. Pemilihan peserta didasarkan pada kebutuhan peningkatan pemahaman mengenai hoaks, perlindungan data pribadi, serta phishing dan penipuan digital.

Tahap pertama adalah identifikasi permasalahan dan kebutuhan melalui observasi awal terhadap pemahaman peserta mengenai penggunaan teknologi dan risiko digital dalam kehidupan sehari-hari. Identifikasi difokuskan pada kemampuan mengenali hoaks, memahami data pribadi yang perlu dilindungi, serta mengenali phishing dan penipuan digital (Lubis et al., 2025). Hasil identifikasi menjadi dasar penyusunan materi dan simulasi yang sesuai dengan kondisi peserta.

Tahap kedua adalah perencanaan dan penyusunan materi yang mencakup tiga aspek, yaitu pengenalan hoaks, perlindungan data pribadi, serta phishing dan penipuan digital. Materi hoaks meliputi ciri informasi mencurigakan dan cara memverifikasi informasi menggunakan prinsip "Berhenti–Periksa–Bagikan". Materi perlindungan data pribadi mencakup jenis data yang perlu dijaga serta langkah pengamanan akun (Rista Ayu Mawarti, 2024). Materi phishing mencakup modus penipuan melalui pesan, telepon, tautan, dan file atau aplikasi dari sumber tidak dikenal. Penyampaian materi menggunakan presentasi, leaflet, contoh kasus, dan simulasi.

Tahap ketiga adalah pelaksanaan edukasi dengan pendekatan partisipatif. Kegiatan diawali dengan pre-test, kemudian dilanjutkan dengan penyampaian materi dan diskusi mengenai hoaks, perlindungan data pribadi, serta phishing dan penipuan digital (Mitrin et al., 2025).

Tahap keempat adalah pendampingan dan simulasi. Peserta didampingi fasilitator dalam mengidentifikasi tanda-tanda mencurigakan melalui simulasi pesan hadiah yang mengarahkan pada tautan tertentu dan telepon yang mengatasnamakan pihak bank serta meminta kode OTP. Peserta diarahkan untuk menentukan tindakan yang tepat berdasarkan materi yang telah diberikan (Basmantra & Murdani, 2022).

Tahap kelima adalah monitoring yang dilakukan selama kegiatan melalui pengamatan terhadap keterlibatan peserta dalam diskusi, kemampuan menjawab pertanyaan, dan kemampuan mengikuti simulasi.

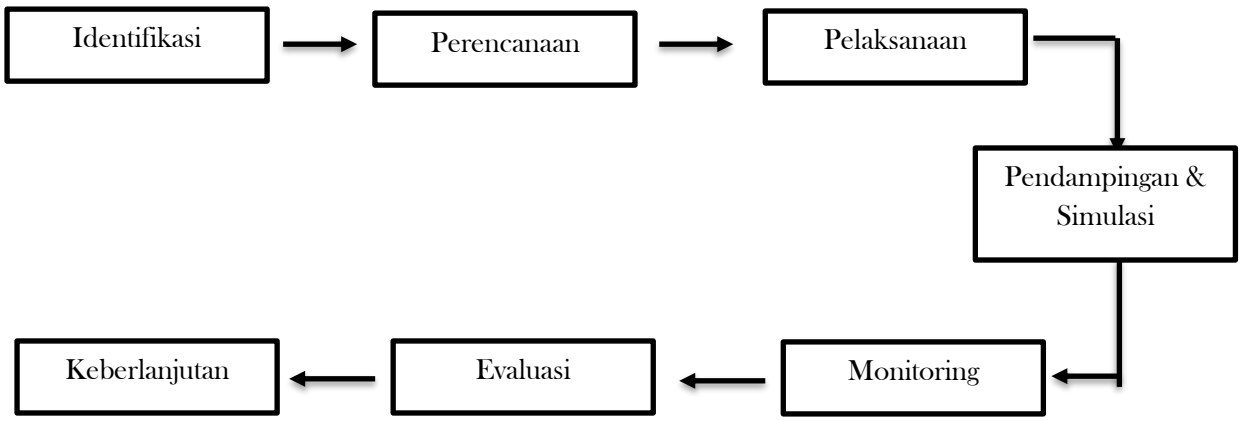
Tahap keenam adalah evaluasi ketercapaian program melalui *pre-test* dan *post-test* yang masing-masing terdiri atas 11 pertanyaan mengenai hoaks, perlindungan data pribadi, serta phishing dan penipuan digital. Instrumen evaluasi berupa pertanyaan tertutup dengan pilihan respons "Ya" dan "Tidak" yang diberikan sebelum dan setelah kegiatan edukasi. Pertanyaan disusun berdasarkan tiga indikator utama. Pada materi hoaks, pertanyaan mengukur pemahaman peserta mengenai ciri-ciri informasi yang meragukan dan pentingnya melakukan pemeriksaan sebelum membagikan informasi. Pada materi perlindungan data pribadi, pertanyaan mengukur pemahaman peserta mengenai jenis data yang perlu dilindungi serta tindakan yang tepat untuk menjaga keamanan data dan akun. Pada materi phishing dan penipuan digital, pertanyaan mengukur pemahaman peserta mengenai ciri-ciri pesan, tautan, atau komunikasi yang mencurigakan serta tindakan yang tepat ketika menghadapinya.

Respons "Ya" menunjukkan bahwa peserta menyatakan telah memahami atau melakukan tindakan yang ditanyakan, sedangkan respons "Tidak" menunjukkan sebaliknya. Setiap respons "Ya" dihitung sebagai satu respons positif, sedangkan respons "Tidak" dihitung sebagai nol. Persentase respons positif dihitung berdasarkan jumlah respons "Ya" dibandingkan dengan jumlah seluruh respons pada setiap tahap evaluasi, kemudian dikalikan 100%. Hasil *pre-test* digunakan untuk menggambarkan kondisi awal pemahaman peserta, sedangkan hasil *post-test* digunakan untuk melihat perubahan respons pemahaman setelah mengikuti edukasi.

Indikator keberhasilan kegiatan ditentukan berdasarkan adanya peningkatan persentase respons "Ya" pada post-test dibandingkan dengan pre-test, baik secara keseluruhan maupun pada masing-masing indikator keamanan digital. Hasil pre-test dan post-test dibandingkan berdasarkan jumlah respons "Ya", persentase respons "Ya", serta perubahan persentase pada setiap indikator. Evaluasi juga didukung melalui observasi selama diskusi dan simulasi untuk melihat keterlibatan

peserta serta respons mereka ketika mengenali ancaman digital dan menentukan tindakan yang tepat (Irwan et al., 2021).

Tahap ketujuh adalah keberlanjutan dengan mendorong peserta menerapkan kebiasaan aman dalam aktivitas digital sehari-hari, terutama menggunakan prinsip "Berhenti–Periksa–Bagikan" serta tidak memberikan data pribadi, kata sandi, PIN, maupun kode OTP kepada pihak lain. Untuk memudahkan pemahaman mengenai tahapan pelaksanaan KKN, berikut gambaran alur pelaksanaannya.



Gambar 1. Alur Pelaksanaan Kegiatan Edukasi Keamanan Digital

HASIL DAN PEMBAHASAN

Pelaksanaan Edukasi dan Pendampingan

Kegiatan edukasi keamanan digital dilaksanakan di Kebon Bawang, RW 09, Kecamatan Tanjung Priok, Jakarta Utara, dengan melibatkan 9 peserta dari masyarakat setempat. Kegiatan difokuskan pada tiga permasalahan utama yang berkaitan dengan aktivitas digital sehari-hari, yaitu kemampuan mengenali hoaks, perlindungan data pribadi, serta pencegahan phishing dan penipuan digital. Pelaksanaan kegiatan dilakukan secara bertahap mulai dari identifikasi kebutuhan, penyampaian materi, pendampingan dan simulasi, monitoring, evaluasi, hingga tindak lanjut keberlanjutan.

Berdasarkan hasil identifikasi awal, peserta telah menggunakan smartphone dan berbagai layanan digital dalam aktivitas sehari-hari. Kondisi tersebut menunjukkan bahwa pemahaman mengenai keamanan digital menjadi penting karena penggunaan teknologi memberikan kemudahan dalam memperoleh informasi dan berkomunikasi, tetapi juga dapat menghadirkan risiko berupa penyebaran informasi palsu, penyalahgunaan data pribadi, serta penipuan melalui media digital (Watrianthos et al., 2022).

Materi edukasi disampaikan menggunakan presentasi dan leaflet dengan bahasa yang sederhana serta contoh yang dekat dengan kehidupan sehari-hari peserta. Materi mencakup ciri-ciri informasi yang patut dicurigai sebagai hoaks, pentingnya memeriksa informasi sebelum mempercayai atau membagikannya, jenis data pribadi yang perlu dilindungi, serta ciri-ciri phishing dan penipuan digital. Salah satu prinsip yang diperkenalkan adalah "Berhenti–Periksa–Bagikan", yaitu membiasakan peserta untuk tidak langsung mempercayai atau menyebarkan informasi sebelum memeriksa sumber dan kebenarannya (Hamzah, 2022).

Pendampingan dilanjutkan melalui simulasi kasus. Peserta diberikan contoh pesan hadiah yang mengarahkan penerima untuk membuka tautan tertentu serta contoh telepon yang mengatasnamakan pihak bank dan meminta kode OTP. Peserta kemudian diminta mengenali tanda-tanda yang mencurigakan dan menentukan tindakan yang tepat. Simulasi tersebut memberikan

kesempatan kepada peserta untuk menghubungkan materi dengan situasi yang menyerupai pengalaman penggunaan media digital sehari-hari (Fathira et al., 2024).

Hasil Evaluasi *Pre-test* dan *Post-test*

Evaluasi dilakukan sebelum dan sesudah kegiatan menggunakan 11 pertanyaan tertutup dengan pilihan respons "Ya" dan "Tidak" yang mencakup tiga indikator, yaitu pengenalan hoaks, perlindungan data pribadi, serta phishing dan penipuan digital. Respons "Ya" menunjukkan bahwa peserta menyatakan telah memahami atau melakukan tindakan yang ditanyakan, sedangkan respons "Tidak" menunjukkan sebaliknya. Setiap respons "Ya" dihitung sebagai satu respons positif, sedangkan respons "Tidak" dihitung sebagai nol. Persentase pemahaman dihitung berdasarkan jumlah respons "Ya" dibandingkan dengan jumlah seluruh respons pada setiap tahap evaluasi. Hasil pre-test dan post-test kemudian dibandingkan untuk melihat perubahan respons pemahaman peserta setelah mengikuti kegiatan edukasi. Hasil evaluasi secara keseluruhan disajikan pada tabel berikut ini.

Keberhasilan kegiatan dilihat dari adanya peningkatan persentase respons "Ya" pada post-test dibandingkan dengan pre-test, baik secara keseluruhan maupun berdasarkan masing-masing indikator.

Tabel 1. Hasil Respons Peserta pada *Pre-test* dan *Post-test*

Evaluasi	Jumlah Respons	Jumlah Seluruh Pertanyaan	Persentase
	Ya		
Pre-Test	95	99	95,96%
Post-Test	99	99	100%
Peningkatan	4	99	4,04 Poin Persentase

Sumber: Data evaluasi kegiatan, 2026.

Berdasarkan Tabel 1, pada pre-test terdapat 95 respons "Ya" dari 99 keseluruhan respons atau sebesar 95,96%. Setelah kegiatan edukasi, seluruh peserta memberikan respons "Ya" pada seluruh pertanyaan sehingga diperoleh 99 respons "Ya" atau 100%. Dengan demikian, terdapat peningkatan sebesar 4,04 poin persentase setelah kegiatan edukasi.

Peningkatan tersebut menunjukkan adanya perubahan respons yang dilaporkan peserta setelah memperoleh edukasi. Meskipun peningkatannya secara keseluruhan relatif kecil, kondisi tersebut berkaitan dengan tingkat pemahaman awal peserta yang sudah cukup tinggi. Artinya, kegiatan tidak dimulai dari kondisi peserta yang sama sekali belum memahami keamanan digital, tetapi lebih banyak berfungsi untuk memperkuat pemahaman yang telah dimiliki dan melengkapi pemahaman pada aspek tertentu yang masih kurang (Almasyhari et al., 2022; Arvita et al., 2025; Fathira et al., 2024; Sopani, 2022).

Tabel 2. Hasil Evaluasi Berdasarkan Indikator

Indikator	Nomor Pertanyaan	Pre-test (%)	Post-test (%)	Peningkatan (poin persentase)
Pengenalan hoaks	1, 3, 4, 5	94,44	100,00	5,56
Perlindungan data pribadi	6, 7, 8, 9, 11	100,00	100,00	0,00
Phishing dan penipuan digital	2, 10	88,89	100,00	11,11
Keseluruhan	**1–11**	**95,96**	**100,00**	**4,04**

Sumber: Data evaluasi kegiatan, 2026.

Berdasarkan Tabel 2, perubahan pemahaman tidak sama pada setiap indikator. Peningkatan terbesar terdapat pada indikator phishing dan penipuan digital, yaitu dari 88,89% menjadi 100% atau

meningkat 11,11 poin persentase. Indikator pengenalan hoaks meningkat dari 94,44% menjadi 100%, sedangkan perlindungan data pribadi tidak menunjukkan perubahan persentase karena sejak pre-test seluruh respons peserta sudah berada pada kategori "Ya".

Hasil tersebut menunjukkan bahwa aspek phishing dan penipuan digital menjadi bagian yang paling membutuhkan penguatan dibandingkan dua indikator lainnya. Pada pre-test, masih terdapat peserta yang memberikan respons "Tidak" pada pertanyaan mengenai pemahaman terhadap phishing, sedangkan pada pertanyaan mengenai perlindungan data pribadi seluruh peserta telah memberikan respons positif. Perbedaan tersebut dapat menunjukkan bahwa istilah dan bentuk phishing relatif kurang familiar bagi sebagian peserta dibandingkan konsep menjaga data pribadi. Setelah diberikan contoh pesan hadiah, tautan mencurigakan, serta permintaan kode OTP melalui simulasi, pemahaman pada indikator tersebut meningkat hingga seluruh peserta memberikan respons positif.

Pada indikator hoaks, peningkatan sebesar 5,56 poin persentase menunjukkan adanya penguatan terhadap kemampuan peserta dalam mengenali informasi yang patut dicurigai. Sebagian besar peserta sebenarnya telah memiliki pemahaman awal yang baik, tetapi masih terdapat respons "Tidak" pada pertanyaan mengenai ciri-ciri hoaks. Pemberian prinsip "Berhenti–Periksa–Bagikan" membantu memperjelas bahwa menerima informasi tidak berarti informasi tersebut langsung dapat dipercaya atau disebarkan. Peserta diarahkan untuk memeriksa sumber dan kebenaran informasi terlebih dahulu.

Sementara itu, tidak adanya peningkatan pada indikator perlindungan data pribadi bukan berarti materi tersebut tidak memberikan manfaat. Seluruh peserta telah memberikan respons positif sejak pre-test, sehingga ruang peningkatannya memang terbatas. Temuan ini justru menunjukkan bahwa peserta telah memiliki kesadaran awal mengenai pentingnya menjaga NIK, nomor KTP, password, PIN, OTP, nomor telepon, email, dan alamat rumah. Edukasi pada indikator ini berfungsi untuk memperkuat pemahaman yang telah dimiliki agar peserta dapat menghubungkannya dengan situasi penipuan digital yang lebih konkret.

Pembahasan

Perbedaan peningkatan pada ketiga indikator menunjukkan bahwa kebutuhan edukasi keamanan digital peserta tidak sepenuhnya sama. Peserta telah memiliki pemahaman awal yang relatif tinggi mengenai perlindungan data pribadi, tetapi pemahaman mengenai phishing dan penipuan digital masih membutuhkan penguatan. Kondisi tersebut menunjukkan pentingnya menyesuaikan materi edukasi dengan jenis risiko yang paling dekat dengan kesulitan peserta, bukan hanya memberikan informasi keamanan digital secara umum.

Peningkatan terbesar pada indikator phishing dan penipuan digital dapat dikaitkan dengan penggunaan contoh yang konkret selama kegiatan. Peserta diberikan situasi berupa pesan hadiah yang mengarahkan pada tautan tertentu dan telepon yang mengatasnamakan pihak bank serta meminta kode OTP. Contoh tersebut membuat konsep phishing tidak hanya dijelaskan sebagai istilah, tetapi diperlihatkan melalui bentuk komunikasi yang dapat ditemui dalam kehidupan sehari-hari (Ramli et al., 2023). Peserta kemudian diarahkan untuk mengenali tanda mencurigakan dan menentukan tindakan yang tepat. Dengan cara tersebut, materi menjadi lebih mudah dihubungkan dengan pengalaman penggunaan smartphone peserta.

Gambar 1. Dokumentasi Kegiatan

Pada indikator hoaks, prinsip "Berhenti–Periksa–Bagikan" memberikan langkah sederhana yang dapat digunakan ketika peserta menerima informasi yang belum diketahui kebenarannya. Peningkatan respons pada indikator ini menunjukkan adanya penguatan terhadap pemahaman mengenai pentingnya melakukan pemeriksaan sebelum menyebarkan informasi. Dengan demikian, edukasi tidak hanya menjelaskan risiko hoaks, tetapi memberikan langkah praktis yang dapat digunakan peserta ketika menghadapi informasi mencurigakan.

Gambar 2. Penyampaian Prinsip "Berhenti–Periksa–Bagikan" dalam Edukasi Hoaks

Temuan kegiatan ini memperkuat hasil kegiatan pengabdian sebelumnya yang menunjukkan pentingnya edukasi keamanan digital dalam meningkatkan pemahaman masyarakat terhadap berbagai risiko penggunaan teknologi. Namun, hasil kegiatan ini memberikan gambaran yang lebih spesifik mengenai perbedaan kebutuhan pemahaman pada tiga jenis risiko digital. Peningkatan terbesar pada phishing dan penipuan digital menunjukkan bahwa materi yang disertai contoh kasus konkret dapat memberikan penguatan yang lebih terlihat pada aspek yang sebelumnya belum terlalu dipahami peserta. Dengan demikian, kegiatan edukasi keamanan digital tidak cukup hanya menyampaikan definisi atau informasi umum, tetapi perlu memberikan contoh yang memungkinkan peserta mengenali dan merespons ancaman secara langsung (Christmas & Vitranilla, 2024).

Hasil evaluasi juga perlu dipahami sesuai dengan karakter instrumen yang digunakan. Respons "Ya" dan "Tidak" menggambarkan pemahaman yang dilaporkan oleh peserta terhadap setiap pertanyaan, sehingga peningkatan dari 95,96% menjadi 100% menunjukkan perubahan respons pemahaman setelah kegiatan. Hasil tersebut belum dapat disamakan dengan bukti perubahan perilaku karena evaluasi tidak mengamati penggunaan media digital peserta dalam jangka panjang. Oleh karena itu, kegiatan ini dapat dikatakan menunjukkan peningkatan pemahaman peserta, tetapi belum dapat digunakan untuk menyimpulkan bahwa kegiatan telah menghasilkan perubahan perilaku keamanan digital secara berkelanjutan.

***Monitoring* dan Faktor Pendukung serta Penghambat**

Monitoring dilakukan selama kegiatan melalui pengamatan terhadap keterlibatan peserta dalam diskusi, respons terhadap pertanyaan, dan kemampuan mengikuti simulasi kasus (Gunawan et al., 2025). Peserta diberikan kesempatan untuk menyampaikan pengalaman atau pertanyaan mengenai pesan mencurigakan, permintaan data pribadi, serta tautan yang diterima melalui media digital. Interaksi tersebut membantu fasilitator memberikan penjelasan yang lebih sesuai dengan kondisi dan pengalaman peserta.

Gambar 3. Dokumentasi Pelaksanaan *Monitoring* Peserta

Beberapa faktor mendukung pelaksanaan kegiatan, antara lain peserta telah terbiasa menggunakan smartphone sehingga contoh kasus dapat dikaitkan dengan aktivitas digital sehari-hari. Penggunaan bahasa sederhana, leaflet, diskusi, dan simulasi juga membantu menyampaikan materi yang bersifat praktis. Pendekatan partisipatif memberikan kesempatan kepada peserta untuk bertanya dan menyampaikan pengalaman secara langsung (Arvita et al., 2025).

Adapun keterbatasan kegiatan terletak pada jumlah peserta yang relatif sedikit dan waktu pelaksanaan yang terbatas. Selain itu, instrumen evaluasi yang digunakan mengukur respons pemahaman peserta melalui pertanyaan "Ya" dan "Tidak", sehingga hasilnya belum dapat menggambarkan kemampuan peserta secara mendalam pada seluruh situasi keamanan digital. Evaluasi juga dilakukan segera setelah kegiatan sehingga belum dapat menunjukkan apakah pemahaman tersebut bertahan dan diterapkan dalam perilaku peserta dalam jangka panjang. Evaluasi lanjutan setelah beberapa waktu dapat digunakan untuk mengetahui keberlanjutan pemahaman dan penerapan kebiasaan keamanan digital.

Dampak, Kebaruan, dan Keberlanjutan Program

Hasil evaluasi menunjukkan adanya peningkatan pemahaman peserta secara keseluruhan dari 95,96% pada pre-test menjadi 100% pada post-test. Peningkatan paling terlihat pada pemahaman mengenai phishing dan penipuan digital. Secara praktis, hasil tersebut menunjukkan bahwa edukasi

memberikan penguatan terhadap kemampuan peserta dalam mengenali risiko digital, khususnya ketika menghadapi pesan, tautan, atau komunikasi yang mencurigakan.

Prinsip "Berhenti–Periksa–Bagikan" menjadi salah satu pendekatan sederhana yang dapat diterapkan peserta ketika menerima informasi yang belum diketahui kebenarannya. Peserta juga diarahkan untuk menjaga kerahasiaan password, PIN, dan kode OTP serta tidak memberikan data pribadi kepada pihak yang tidak berkepentingan (Rosihan & Novitasari, 2022). Meskipun demikian, penerapan kebiasaan tersebut dalam kehidupan sehari-hari belum dapat dipastikan berdasarkan hasil evaluasi ini karena perubahan perilaku tidak diukur setelah kegiatan.

Unsur kebaruan kegiatan terletak pada penggabungan edukasi mengenai hoaks, perlindungan data pribadi, serta phishing dan penipuan digital dalam satu rangkaian pembelajaran yang berorientasi pada situasi sehari-hari masyarakat. Kegiatan tidak hanya menyampaikan materi, tetapi juga menggunakan contoh kasus, diskusi, dan simulasi sehingga peserta memperoleh kesempatan untuk mengenali risiko dan menentukan tindakan yang tepat. Pendekatan tersebut memberikan pengalaman belajar yang lebih aplikatif dibandingkan edukasi yang hanya berfokus pada penyampaian informasi secara satu arah (Irwan et al., 2021).

Keberlanjutan program diarahkan pada penerapan kebiasaan keamanan digital oleh peserta dalam aktivitas sehari-hari. Peserta diharapkan dapat menggunakan prinsip "Berhenti–Periksa–Bagikan" ketika menerima informasi, memeriksa sumber sebelum membagikannya, menjaga kerahasiaan data pribadi, serta menghindari tautan dan permintaan data yang mencurigakan. Dengan demikian, hasil kegiatan dapat menjadi dasar bagi peserta untuk membangun kebiasaan penggunaan media digital yang lebih aman. Evaluasi lanjutan secara berkala diperlukan untuk mengetahui apakah pemahaman yang diperoleh dapat dipertahankan dan diterapkan dalam perilaku digital sehari-hari.

KESIMPULAN

Kegiatan KKN dalam rangka edukasi keamanan digital di Kebon Bawang, RW 09, Kecamatan Tanjung Priok, Jakarta Utara pada 10 Agustus 2026 menunjukkan adanya peningkatan pemahaman peserta mengenai keamanan digital. Berdasarkan hasil evaluasi terhadap 9 peserta dengan 11 pertanyaan tertutup, respons "Ya" meningkat dari 95 dari 99 respons pada *pre-test* (95,96%) menjadi 99 dari 99 respons pada *post-test* (100%), atau meningkat sebesar 4,04 poin persentase. Berdasarkan indikator, peningkatan terbesar terdapat pada materi phishing dan penipuan digital, yaitu dari 88,89% menjadi 100% atau meningkat 11,11 poin persentase, sedangkan pengenalan hoaks meningkat dari 94,44% menjadi 100% atau 5,56 poin persentase. Pada indikator perlindungan data pribadi, persentase respons "Ya" tetap 100% pada *pre-test* dan *post-test*. Hasil tersebut menunjukkan bahwa kegiatan edukasi, diskusi, leaflet, dan simulasi kasus dapat mendukung penguatan pemahaman peserta, terutama pada aspek yang masih membutuhkan perhatian seperti pengenalan phishing dan penipuan digital.

Kegiatan ini juga menunjukkan bahwa edukasi keamanan digital dapat disampaikan melalui pendekatan yang sederhana, partisipatif, dan berbasis situasi yang dekat dengan penggunaan media digital sehari-hari. Pengenalan prinsip "Berhenti–Periksa–Bagikan", perlindungan data pribadi, serta kewaspadaan terhadap tautan dan permintaan informasi yang mencurigakan menjadi bagian praktis yang dapat diterapkan peserta dalam aktivitas digital. Namun, evaluasi kegiatan memiliki keterbatasan karena instrumen yang digunakan berupa pertanyaan tertutup dengan respons "Ya" dan "Tidak" yang mengukur pemahaman yang dilaporkan peserta, serta *post-test* dilakukan segera setelah kegiatan. Dengan demikian, hasil evaluasi belum dapat menggambarkan perubahan perilaku, keterampilan, maupun keberlanjutan penerapan keamanan digital dalam jangka panjang. Kegiatan selanjutnya dapat menggunakan instrumen pengetahuan yang lebih objektif, simulasi yang lebih beragam, dan evaluasi lanjutan untuk melihat perubahan pemahaman dan keterampilan peserta secara lebih akurat.

UCAPAN TERIMA KASIH

Kami panjatkan rasa Syukur kami kepada Tuhan YME atas segala rahmat dalam acara ini. Kami juga menyampaikan terima kasih kepada Universitas 17 Agustus 1945 Jakarta yang telah mendukung pelaksanaan kegiatan Kuliah Kerja Nyata (KKN) sebagai bagian dari kegiatan pengabdian kepada masyarakat serta mendukung proses penyusunan artikel ini. Ucapan terima kasih juga disampaikan kepada masyarakat Kebon Bawang, RW 9, Kecamatan Tanjung Priok, Jakarta Utara, yang telah berpartisipasi dan mendukung pelaksanaan kegiatan edukasi keamanan digital sehingga kegiatan dapat terlaksana dengan baik. Terakhir, terima kasih kepada teman-teman KKN Kelompok 8 Sore atas kerja sama, partisipasi, dan dukungan selama proses pelaksanaan kegiatan hingga penyusunan jurnal pengabdian ini.

DAFTAR PUSTAKA

Almasyhari, A. K., Sari, Y. P., & Sukesti, F. (2022). Edukasi Literasi Digital: Peningkatan Kesadaran Masyarakat Dalam Perlindungan Data Pribadi Dan Kaitannya Terhadap Financial Technology. *Jurnal Pengabdian Masyarakat Progresif Humanis Brainstorming*, *5*(3), 449–453. Https://Doi.Org/10.30591/Japhb.V5i3.3849

Alpayed, D., Jabbar, A. A., Salsabila, A. A., & Mahmudin, A. A. (2025). Tingkat Literasi Digital Mahasiswa Generasi Z Program Studi Pendidikan Bahasa Arab Dalam Mengidentifikasi Dan Mengatasi Hoaks Di Media Sosial. *Jurnal Literasi Digital*, *5*(1), 86–95. Https://Doi.Org/10.54065/Jld.5.1.2025.796

Arvita, Y., Arief, M., Sutoyo, H., Riyadi, W., & Hartiwi, Y. (2025). Sosialisasi Literasi Dan Kemanan Digital Bagi Siswa / I Sma Negeri 3 Kota Jambi. *Jurnal Pengabdian Masyarakat Unama (Jpmu)*, *2*(1), 36–41. Https://Doi.Org/10.33998/Jpmu.V2i1

Basmantra, I. N., & Murdani, N. L. G. P. (2022). Literasi digital dalam mengatasi berita palsu (hoaks) Covid-19 pada masyarakat Desa Adat Kampial. *GERVASI: Jurnal Pengabdian kepada Masyarakat*, *6*(2), 387–397. https://doi.org/10.31571/gervasi.v6i2.3476

Christmas, S. K., Vitranilla, Y. E., Ramadhania, W., Angelina, P., & Akbar, M. F. (2024). Pendidikan keamanan data: Perlindungan hukum terhadap mitigasi pencurian data dengan pemanfaatan artificial intelligence berbasis SDGs. *Sang Sewagati Journal*, *2*(2), 73–84. https://doi.org/10.37253/sasenal.v2i2.10296

Dinihari, Y., Wiyanti, E., Nazelliana, D., Karyati, Z., Lutfi, L., & Handayani, W. (2025). Discourse Analysis Of Digital Hoaxes As A Critical Literacy Strategy In Indonesian Language Education. *Kembara Journal Of Scientific Language Literature And Teaching*, *11*(1), 185–198. Https://Doi.Org/10.22219/Kembara.V11i1.40485

Fathira, V., Zuriati, D., Maspufah, M., Asril, L. Z., Putri, N. A. J., & Anjelia, R. (2024). Membangun kesadaran literasi digital dan kecerdasan dalam menangkal hoaks pada siswa SMA IT Fadhilah. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(12), 3346–3353. https://doi.org/10.59837/jpmba.v1i11.722

Gunawan, G., Ujianto, N. T., Andriani, W., & Firmansyah, H. (2025). Transformasi Literasi Digital Dalam Pendidikan Vokasi Untuk Perlindungan Privasi Dan Keamanan Siber Di Smk Astrindo Kota Tegal ,. *Jurnal Pengabdian Masyarakat Terapan (Jupiter*, *2*(2), 63–72. Https://Doi.Org/10.20884/1.Jupiter.2.2.69

Hamzah, A. (2022). Peningkatan Literasi Digital Untuk Mencegah Penyebaran Hoax Bagi Guru Sdn Teruman Bantul. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, *2*(2), 92–97. Https://Doi.Org/10.25008/Abdiformatika.V2i2.168

Illahi, S. M., & Rita Gani. (2024). Hubungan Literasi Media Digital Dengan Penyebaran Hoax Di Kalangan Generasi Z. *Jurnal Riset Jurnalistik Dan Media Digital*, *1*, 183–188. Https://Doi.Org/10.29313/Jrjmd.V4i2.5042

Irwan, I., Azmi, A., Syafril, R., & Tiara, M. (2021). Pemberdayaan aparatur pemerintahan nagari melalui

literasi digital anti-hoaks dan penguatan ketahanan informasi nagari. *Abdi: Jurnal Pengabdian dan Pemberdayaan Masyarakat*, *3*(2), 209–214. https://doi.org/10.24036/abdi.v3i2.165

Istoningtyas, M., Astri, L. Y., Irawan, B., & Irawan. (2023). Literasi Digital Perlindungan Data Pribadi "Kita Butuh Privasi" Untuk Siswa/I Sma N 7 Muaro Jambi. *Jurnal Pengabdian Masyarakat Unama*, *2*(2), 1–6. Https://Doi.Org/10.33998/Jpmu.2023.2.2.1456

Kominfo. (2025). *Peluncuran Hasil Pengukuran Indeks Masyarakat Digital Indonesia (Imdi) Tahun 2024*. Komdigi.Go.Id. Https://Bpsdm.Komdigi.Go.Id/Berita-Peluncuran-Hasil-Pengukuran-Indeks-Masyarakat-Digital-Indonesia-Imdi-Tahun--46-2092?Utm_Source=Chatgpt.Com

Krisnawati, I., Hasrul, H., Fatmariza, F., & Indrawadi, J. (2023). Pelaksanaan Program Literasi Digital Untuk Menanggulangi Berita Hoaks. *Journal Of Education, Cultural And Politics*, *3*(2), 313–324. Https://Doi.Org/10.24036/Jecco.V3i2.103

M.T, R., Yusran, Y., & Maulidia, C. A. (2022). Analisis Pemahaman Literasi Digital Pada Mahasiswa Uin Arraniry Terhadap Digital Skill Dan Digital Safety. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *6*(2), 142–148. Https://Doi.Org/10.22373/Cj.V6i2.15433

Mawarti, R. A., Hanafi, H., & Agung, L. P. (2024). Optimalisasi rancangan desa pintar melalui peningkatan literasi kewargaan Karang Taruna di bidang penangkalan berita palsu. *PengabdianMu: Jurnal Ilmiah Pengabdian kepada Masyarakat*, *9*(12), 2381–2388. https://doi.org/10.33084/pengabdianmu.v9i12.8359

Mitrin, A., Kurniawan, B., & Rahman, R. (2025). PKM penguatan kapasitas masyarakat dalam mencegah hoaks digital melalui pengenalan teknologi deepfake dan deteksi hoaks menggunakan data science di Karang Taruna Kecamatan Kerinci Kanan. *Jurnal Pengabdian Masyarakat (ABDIRA)*, *5*(4), 751–763. https://doi.org/10.31004/abdira.v5i4.112

Prasetyo, H., Kameliani, K., Wildan, W., Rasya, A., & Tutu, A. P. (2026). Sosialisasi cyber security awareness: Mitigasi phishing dan pengamanan akun digital bagi siswa SMA/SMK. *Empiris Jurnal Pengabdian Pada Masyarakat*. https://doi.org/10.59713/fh9by653

Purnama, H., Astuti, S. W., Imran, A. I., & Devi, S. G. N. P. (2024). Literasi Digital Safety Bagi Anggota Pramuka Kwarcab Kota Bandung. *Jurnal Pengabdian Masyarakat Bangsa*, *2*(5), 1279–1286. Https://Doi.Org/10.59837/Jpmba.V2i5.991

Putri Silmina, E., Sarmin, S., Umar, R., & Herman, H. (2025). Meningkatkan Literasi Digital: Perlindungan Data Pribadi Dan Pencegahan Penipuan Online Di Lingkungan Pra Ngadisuryan. *Jurnal Pengabdian Untukmu Negeri*, *9*(2), 322–330. Https://Doi.Org/10.37859/Jpumri.V9i2.9860

Putri, A. D. P., Mahpudin, A. S., & Fadhilah, D. (2025). Literasi Digital Sebagai Tanggung Jawab Sosial Dalam Menangkal Hoaks. *Jurnal Literasi Digital*, *5*(1), 110–120. Https://Doi.Org/10.54065/Jld.5.1.2025.797

Rahajoe, A. D., & Setyatama, F. (2022). Sosialisasi literasi digital dalam rangka penguatan peran masyarakat menangkal hoaks (studi kasus: Petugas TBM Surabaya). *Jurnal Abdi Bhayangkara*, *4*(2), 917–930. https://doi.org/10.55499/jab.vi.1332

Rosihan, A., & Novitasari, D. (2022). Literasi digital bagi remaja dan Karang Taruna dalam upaya mencegah informasi hoax di Desa Sukaraja Kecamatan Lengkiti Kabupaten Ogan Komering Ulu. *Wahana Dedikasi: Jurnal PkM Ilmu Kependidikan*, *5*(2), 11–20. https://doi.org/10.31851/dedikasi.v5i2.7536

Siti Mutmainah, Teguh Ansor Lorosae, Alamin, Z., & Sutriawan. (2025). Pelatihan Literasi Digital Dan Pengelolaan Data Pribadi Untuk Remaja Di Era Big Data. *Jurnal Sosiall Masyarakat*, *2*(2), 56–64. Https://Doi.Org/10.63866/Pemas.V2i2.74

Sopani, I. (2022). Literasi Digital Dalam Menghadapi Hoaks Di Masa Pandemi. *Deiksis: Jurnal Pendidikan Bahasa Dan Sastra Indonesia*, *9*(1), 36–44. Https://Doi.Org/10.33603/Deiksis.V9i1.6238

Utomo, F. W., Mauludin Insana, D. R., & Mayndarto, E. C. (2024). Mekanisme Penipuan Digital Pada Masyarakat Era 5.0 (Studi Kasus Penipuan Online Berbasis Lowongan Kerja Paruh Waktu

Yang Merebak Di Masyarakat). *Jurnal Ilmiah Wuny*, *6*(1), 32–41. Https://Doi.Org/10.21831/Jwuny.V6i1.72257

Wahyu Hidayat M., Ramli, H., Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Junedy, R. (2023). Analisa clustering phising untuk meningkatkan kesadaran mahasiswa terhadap keamanan data pribadi mahasiswa Universitas Negeri Makassar. *Vokatek: Jurnal Pengabdian Masyarakat*, *1*(1), 28–33. https://doi.org/10.61255/vokatekjpm.v1i1.29

Watrianthos, R., Samsir, Harahap, J. M., Ramadhana, R. S. A., & Marpaung, M. F. R. (2022). Pelatihan literasi digital bagi siswa MTs Ar-Royan Pangkatan untuk mencegah hoax di sosial media. *REKA KARYA: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 144–150. https://doi.org/10.26760/rekakarya.v1i2.145-150

Wirajaya, M. K. M., Jaya, P. P., Aryanata, N. T., Tunas, I. K., Rettobjaan, V. F. C., Yudha, A. A. N. B. A., & Widyani, N. M. (2024). Sosialisasi Literasi Digital Tentang Cakap Mengenali Hoaks Dan Keamanan Ruang Digital Pada Sekaa Teruna Di Desa Gunung Sari, Kabupaten Buleleng. *Jurnal Pelayanan Dan Pengabdian Masyarakat (Pamas)*, *8*(3), 210–216. Https://Doi.Org/10.52643/Pamas.V8i3.2693

Zalukhu, A. I., Gloria, M. D., Hulu, A. P. H., Syahputra, I., Zalukhu, R. N. Y., & Zalukhu, D. K. (2026). Edukasi Pencegahan Phishing Sebagai Upaya Peningkatan Kesadaran Keamanan Digital. *Jurnal Pengabdian Masyarakat Variasi*, *3*(1), 1-6. https://doi.org/10.36520/jpmv.v3.i1.123