

Peningkatan Kesadaran Keamanan Siber melalui Edukasi Bahaya Link Phishing pada Generasi Y

Erik Amanda Putri Aprilia¹, Atika Risky Cahyani^{2*}, Fitriana Novitasari³

¹⁻³Universitas Negeri Yogyakarta, Indonesia

*Penulis korespondensi, email: atikarisky.2024@student.uny.ac.id

Abstrak— Perkembangan teknologi digital yang pesat meningkatkan penggunaan internet di kalangan masyarakat, namun turut meningkatkan risiko kejahatan siber, termasuk serangan phishing, khususnya pada kelompok Generasi Y yang memiliki intensitas penggunaan internet tinggi. Kegiatan pengabdian ini bertujuan meningkatkan kesadaran keamanan siber melalui edukasi bahaya tautan phishing pada anggota komunitas Generasi Y. Kegiatan menggunakan pendekatan deskriptif kuantitatif dengan desain pre-test dan post-test, melibatkan 30 orang dewasa Generasi Y yang aktif menggunakan ponsel pintar untuk komunikasi, media sosial, pencarian informasi, dan transaksi digital sebagai sasaran kegiatan. Edukasi dilakukan melalui presentasi, diskusi, dan sesi tanya jawab yang mencakup definisi phishing, karakteristik tautan phishing, dampak potensial, metode pencegahan, dan praktik keamanan digital. Hasil menunjukkan peningkatan pemahaman yang signifikan setelah intervensi edukasi, yaitu pengetahuan tentang phishing meningkat dari 13,33% menjadi 100%, pemahaman keamanan OTP meningkat dari 0% menjadi 100%, dan kesadaran terhadap tautan mencurigakan meningkat dari 0% menjadi 93,33%. Temuan ini menunjukkan bahwa edukasi keamanan siber efektif meningkatkan literasi digital dan kesadaran masyarakat terhadap ancaman siber, sehingga dapat direkomendasikan sebagai strategi berkelanjutan untuk mengurangi risiko masyarakat, khususnya Generasi Y, menjadi korban kejahatan siber.

Kata kunci: keamanan siber; literasi digital; pendidikan siber; phishing; tautan phishing.

This article is licensed under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah memberikan berbagai kemudahan bagi masyarakat dalam menjalankan aktivitas sehari-hari. Bagi Generasi Y, internet tidak hanya digunakan sebagai sarana komunikasi, tetapi juga sebagai media untuk memperoleh informasi, mengakses layanan publik, melakukan transaksi keuangan, serta berinteraksi melalui berbagai platform digital. Perkembangan teknologi digital tersebut ternyata juga menimbulkan berbagai ancaman keamanan siber yang dapat merugikan pengguna. Meningkatnya penggunaan teknologi digital menyebabkan risiko kejahatan siber semakin tinggi, baik dalam bentuk pencurian data, penyalahgunaan informasi pribadi, maupun penipuan digital yang dilakukan melalui media internet.

Generasi Y atau milenial merupakan salah satu kelompok masyarakat yang aktif menggunakan teknologi digital. Generasi ini lahir dan tumbuh pada masa perkembangan teknologi informasi sehingga memiliki tingkat penggunaan internet yang cukup tinggi dalam berbagai aktivitas sehari-hari, seperti komunikasi, transaksi digital, penggunaan media sosial, dan pencarian informasi [1]. Tingginya intensitas penggunaan

teknologi tersebut menjadikan Generasi Y memiliki peluang yang lebih besar untuk terpapar berbagai ancaman keamanan siber, termasuk phishing. Peningkatan kesadaran keamanan siber pada Generasi Y menjadi penting untuk dilakukan agar kelompok ini mampu menggunakan teknologi digital secara aman dan bertanggung jawab.

Keamanan siber menjadi aspek penting dalam era digital karena meningkatnya penggunaan teknologi informasi turut diikuti oleh berbagai ancaman siber, seperti hacking, phishing, dan malware. Ancaman tersebut dapat menyebabkan kebocoran data pribadi, pencurian identitas, serta kerugian finansial bagi pengguna sehingga diperlukan upaya perlindungan data yang lebih efektif [2]. Keamanan siber merupakan upaya perlindungan terhadap sistem, jaringan, perangkat, dan data dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi [3]. Keamanan data menjadi salah satu aspek penting dalam keamanan siber karena berkaitan dengan perlindungan informasi pribadi dari akses yang tidak sah maupun penyalahgunaan oleh pihak yang tidak bertanggung jawab, sehingga tidak hanya melibatkan penggunaan teknologi tetapi juga kesadaran pengguna dalam menjaga informasi yang dimiliki.

Salah satu bentuk kejahatan siber yang sering terjadi di masyarakat luas adalah phishing. Phishing merupakan metode penipuan yang dilakukan dengan memanfaatkan tautan atau situs palsu untuk memperoleh informasi sensitif milik pengguna, seperti kata sandi, kode OTP, data perbankan, maupun identitas pribadi lainnya [4]. Modus phishing pada media sosial umumnya dilakukan dengan menjebak pengguna melalui tautan yang meyakinkan maupun melalui pesan surel, sehingga korban secara tidak sadar memberikan data pribadinya kepada pelaku [5]. Serangan phishing memanfaatkan ketidaktahuan atau kurangnya kewaspadaan pengguna internet sehingga korban secara sukarela memberikan informasi yang diminta oleh pelaku, dan akibatnya korban dapat mengalami kerugian berupa pencurian akun, penyalahgunaan data pribadi, sampai kerugian finansial. Peningkatan pemahaman masyarakat tentang phishing menjadi salah satu langkah penting dalam mencegah terjadinya kejahatan siber.

Upaya peningkatan kesadaran masyarakat terhadap keamanan digital dapat dilakukan melalui penguatan literasi digital. Literasi digital tidak hanya berkaitan dengan kemampuan menggunakan perangkat teknologi, tetapi juga kemampuan dalam mengakses, memahami, mengevaluasi, dan menggunakan informasi secara aman serta bertanggung jawab [1]. Individu yang memiliki literasi digital yang baik akan lebih mampu mengenali informasi yang berpotensi membahayakan, termasuk tautan phishing yang sering beredar melalui media sosial, email, maupun aplikasi pesan instan (SMS). Literasi digital dengan demikian memiliki peran penting dalam membentuk perilaku masyarakat yang lebih bijak dan aman dalam menggunakan teknologi digital.

Penelitian mengenai edukasi keamanan digital sudah banyak dilakukan sebelumnya dengan sasaran dan pendekatan yang beragam. Edukasi keamanan digital terbukti memiliki peran penting dalam meningkatkan kewaspadaan masyarakat terhadap serangan phishing melalui tautan palsu, sehingga masyarakat mampu mengenali ciri-ciri phishing serta langkah-langkah pencegahannya [4]. Kegiatan edukasi keamanan siber juga mampu meningkatkan pemahaman masyarakat mengenai berbagai bentuk penipuan digital, perlindungan identitas, serta keamanan perangkat yang digunakan dalam aktivitas sehari-hari [6]. Sosialisasi dan edukasi mengenai keamanan data dan privasi terbukti dapat meningkatkan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi serta mendorong penerapan perilaku digital yang lebih aman [7]. Pelatihan sejenis yang menyasar siswa sekolah dasar juga menunjukkan peningkatan kesadaran keamanan siber setelah pemberian media edukasi interaktif [8], sementara edukasi keamanan siber terhadap ancaman phishing juga terbukti relevan diberikan pada kelompok peserta didik nonformal untuk melindungi data pribadi mereka [9]. Pelatihan kecakapan literasi digital turut terbukti meningkatkan pemahaman etis penggunaan teknologi informasi pada masyarakat umum [10], dan edukasi mengenai etika bermedia sosial yang aman turut berkontribusi pada peningkatan kesadaran keamanan digital masyarakat secara luas [11].

Berbagai penelitian terdahulu tersebut umumnya menasar kelompok pelajar, siswa sekolah, maupun masyarakat umum secara luas, sementara kajian yang secara khusus menasar Generasi Y sebagai kelompok dengan tingkat penggunaan internet yang tinggi masih terbatas jumlahnya. Selain itu, masih sedikit kegiatan yang mengevaluasi peningkatan pemahaman peserta secara terukur melalui pengukuran pre-test dan post-test terkait bahaya phishing. Kebaruan kegiatan ini terletak pada fokus sasaran Generasi Y dewasa serta pada penggunaan desain evaluasi pre-test dan post-test untuk mengukur secara kuantitatif perubahan pemahaman peserta terhadap bahaya link phishing.

Berdasarkan hasil observasi awal dan pre-test yang dilakukan pada peserta kegiatan, masih ditemukan rendahnya tingkat pemahaman mengenai phishing dan keamanan digital. Sebagian peserta belum memahami pengertian phishing secara tepat, belum mengetahui pentingnya menjaga kerahasiaan kode OTP, serta belum mampu mengidentifikasi karakteristik tautan yang mencurigakan. Kondisi tersebut menunjukkan adanya kesenjangan antara tingginya penggunaan teknologi digital dengan tingkat kesadaran keamanan siber masyarakat, sehingga diperlukan upaya edukasi untuk meningkatkan pengetahuan dan kewaspadaan masyarakat terhadap ancaman phishing di lingkungan digital. Kegiatan edukasi mengenai bahaya link phishing ini bertujuan untuk meningkatkan pemahaman dan kesadaran Generasi Y terhadap keamanan siber, dengan efektivitas kegiatan dievaluasi melalui perbandingan hasil pre-test dan post-test.

2. Metode Pelaksanaan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk sosialisasi dan edukasi keamanan siber dengan tema “Waspada Link Phishing: Cara Aman Berinternet di Era Digital”. Kegiatan dilaksanakan di lingkungan mitra yang menjadi tempat berdomisilinya peserta sasaran dari kelompok Generasi Y. Program ini bertujuan meningkatkan pengetahuan dan kesadaran masyarakat mengenai ancaman phishing serta pentingnya menjaga keamanan data pribadi dalam penggunaan internet dan layanan digital.

Peserta kegiatan berjumlah 30 orang yang berasal dari kelompok Generasi Y, terdiri atas ibu-ibu dan bapak-bapak. Sebagian besar peserta menggunakan smartphone dalam aktivitas sehari-hari, seperti berkomunikasi melalui WhatsApp, mengakses media sosial, mencari informasi, serta melakukan transaksi digital. Tingginya intensitas penggunaan teknologi digital tersebut menjadikan peserta rentan terhadap berbagai bentuk kejahatan siber, khususnya penipuan melalui tautan (link) phishing.

Metode yang digunakan adalah metode deskriptif kuantitatif dengan desain pre-test dan post-test. Data diperoleh melalui observasi, kuesioner pre-test, kuesioner post-test, serta dokumentasi kegiatan. Pelaksanaan kegiatan terdiri atas lima tahapan, yaitu observasi awal, pelaksanaan pre-test, penyampaian materi edukasi, sesi diskusi dan tanya jawab, serta pelaksanaan post-test untuk mengukur perubahan tingkat pemahaman peserta. Alur pelaksanaan kegiatan dan dokumentasi pelaksanaan disajikan pada Gambar 1.

Metode pendampingan dilakukan melalui penyampaian materi menggunakan media presentasi berbantuan laptop serta bahan ajar cetak. Materi yang diberikan meliputi pengertian phishing, karakteristik tautan phishing, contoh kasus yang sering terjadi di masyarakat, dampak yang ditimbulkan, langkah-langkah pencegahan, serta pentingnya menjaga kerahasiaan data pribadi di era digital. Penyampaian materi dilakukan secara interaktif dan dilanjutkan dengan sesi diskusi serta tanya jawab untuk memperkuat pemahaman peserta terhadap materi yang disampaikan.

Instrumen evaluasi berupa kuesioner pre-test dan post-test yang memuat pertanyaan mengenai pemahaman phishing, keamanan kode OTP, serta kemampuan mengidentifikasi tautan yang mencurigakan. Data hasil pengukuran dianalisis secara deskriptif menggunakan persentase untuk

mengetahui peningkatan tingkat pemahaman peserta setelah mengikuti kegiatan. Keberhasilan program ditentukan berdasarkan peningkatan persentase jawaban benar pada post-test dibandingkan dengan pre-test pada setiap indikator yang diukur. Ringkasan tahapan pelaksanaan beserta hasil kegiatan disajikan pada Tabel 1. Metode pelaksanaan yang diterapkan diharapkan dapat menjadi model yang mudah direplikasi pada kelompok masyarakat lain dengan karakteristik penggunaan teknologi digital yang serupa.



Gambar 1. Alur Metode Pelaksanaan Kegiatan.

Tabel 1. Ringkasan hasil kegiatan

No	Indikator Kegiatan	Hasil Kegiatan
1	Observasi Awal	Peserta aktif menggunakan smartphone dan internet dalam kegiatan sehari-hari, namun masih memiliki pemahaman yang terbatas mengenai ancaman phishing dan keamanan data pribadi.
2	Pre-Test	Dilakukan pengukuran terhadap pengetahuan awal peserta mengenai phishing, keamanan OTP, dan identifikasi tautan mencurigakan.
3	Penyampaian Materi	Menyampaikan materi kepada peserta terkait phishing, ciri-ciri phishing, dampak, dan langkah pencegahan.
4	Diskusi dan Tanya Jawab	Peserta menunjukkan antusiasme yang tinggi dengan mengajukan pertanyaan dan berbagi pengalaman terkait penipuan digital yang pernah ditemui.
5	Post-Test	Hasil post-test menunjukkan adanya peningkatan pemahaman peserta terkait keamanan siber dan cara mengenali link phishing dibandingkan sebelumnya.
6	Evaluasi Kegiatan	Kegiatan sosialisasi berjalan dengan baik dan mampu meningkatkan kesadaran peserta terkait pentingnya menjaga keamanan data pribadi dan kewaspadaan terhadap ancaman phishing.

3. Hasil dan Pembahasan

Sebanyak 30 peserta mengikuti kegiatan edukasi keamanan siber yang terdiri atas ibu-ibu dan bapak-bapak dari kelompok Generasi Y. Sebagian besar peserta menggunakan smartphone dalam aktivitas sehari-hari, seperti berkomunikasi melalui WhatsApp, mengakses media sosial, mencari informasi, dan melakukan transaksi digital. Karakteristik penggunaan teknologi tersebut menjadikan peserta sebagai kelompok sasaran yang relevan untuk memperoleh edukasi mengenai keamanan siber, khususnya terkait ancaman phishing. Pengalaman awal peserta dalam menerima tautan mencurigakan sebelum pelaksanaan edukasi disajikan pada Tabel 2.

Tabel 2. Pengalaman peserta menerima link mencurigakan

Pengalaman Menerima Link Mencurigakan	Jumlah	Persentase
Ya	13	43,33%
Tidak	17	56,67%

Berdasarkan Tabel 2, sebanyak 13 peserta (43,33%) menyatakan pernah menerima link mencurigakan, sedangkan 17 peserta (56,67%) belum pernah mengalaminya. Temuan tersebut menunjukkan bahwa hampir separuh peserta telah berhadapan dengan potensi ancaman siber sehingga edukasi mengenai identifikasi phishing menjadi sangat relevan.

Selain pengalaman menerima link mencurigakan, pre-test juga digunakan untuk mengukur pengetahuan awal peserta mengenai keamanan siber. Hasil pengukuran tersebut disajikan pada Tabel 3.

Tabel 3. Hasil pre-test pengetahuan keamanan siber

Pertanyaan	Jawaban Benar	Persentase
Memahami phishing	4	13,33%
Memahami keamanan OTP	0	0%
Memahami keamanan link WhatsApp	0	0%
Mengetahui tindakan saat menemukan link mencurigakan	30	100%

Berdasarkan Tabel 3, tingkat pengetahuan awal peserta mengenai keamanan siber masih tergolong rendah. Hanya 13,33% peserta yang memahami pengertian phishing, sedangkan belum ada peserta yang

memahami pentingnya menjaga kerahasiaan kode OTP maupun mengenali keamanan link WhatsApp. Meskipun demikian, seluruh peserta telah mengetahui bahwa tautan mencurigakan perlu diverifikasi terlebih dahulu sebelum dibuka. Kondisi tersebut menunjukkan bahwa peserta telah memiliki kewaspadaan dasar, tetapi belum memahami konsep keamanan siber secara komprehensif.

Selanjutnya, kegiatan edukasi dilaksanakan melalui sosialisasi bertema "Waspada Link Phishing: Cara Aman Berinternet di Era Digital". Materi yang disampaikan meliputi pengertian phishing, karakteristik link phishing, contoh kasus penipuan digital, dampak terhadap korban, langkah-langkah pencegahan, serta pentingnya menjaga kerahasiaan data pribadi, kode OTP, dan kata sandi. Penyampaian materi dilakukan menggunakan media presentasi dan dilanjutkan dengan diskusi interaktif serta sesi tanya jawab. Peserta menunjukkan antusiasme yang tinggi dengan mengajukan pertanyaan dan berbagi pengalaman mengenai pesan maupun tautan mencurigakan yang pernah diterima melalui berbagai platform digital.

Setelah kegiatan selesai, dilakukan post-test untuk mengevaluasi peningkatan pemahaman peserta. Hasil pengukuran tersebut disajikan pada Tabel 4.

Tabel 4. Hasil post-test peserta

Indikator Pengetahuan	Jawaban Benar	Persentase
Memahami bahwa phishing merupakan upaya pencurian data pribadi	30	100%
Mengetahui bahwa kode OTP dan password tidak boleh diberikan kepada orang lain	30	100%
Mengetahui bahwa link mencurigakan tidak boleh langsung dibuka	28	93,33%
Mengetahui pentingnya memverifikasi pesan yang mengatasmakan bank	30	100%
Menjadi lebih berhati-hati saat membuka link setelah edukasi	30	100%

Berdasarkan Tabel 4, terjadi peningkatan pemahaman peserta setelah mengikuti kegiatan edukasi. Seluruh peserta memahami bahwa phishing merupakan upaya pencurian data pribadi, mengetahui pentingnya menjaga kerahasiaan kode OTP dan kata sandi, serta menyadari perlunya memverifikasi pesan yang mengatasmakan institusi resmi sebelum memberikan informasi pribadi. Sebanyak 93,33% peserta juga mampu mengidentifikasi bahwa link mencurigakan tidak boleh langsung dibuka. Perbandingan hasil pre-test dan post-test untuk setiap indikator pengetahuan disajikan pada Tabel 5.

Tabel 5. Perbandingan hasil pre-test dan post-test

Indikator	Pre-Test (%)	Post-Test (%)	Peningkatan (%)
Memahami phishing	13,33%	100%	86,67%
Keamanan OTP	0%	100%	100%
Keamanan link	0%	93,33%	93,33%
Verifikasi pesan mencurigakan	100%	100%	0%

Berdasarkan Tabel 5, seluruh indikator mengalami peningkatan yang signifikan setelah pelaksanaan edukasi. Pemahaman mengenai phishing meningkat sebesar 86,67%, sedangkan pemahaman mengenai keamanan kode OTP meningkat dari 0% menjadi 100%. Kemampuan mengenali link yang mencurigakan juga meningkat hingga mencapai 93,33%. Sementara itu, indikator verifikasi pesan tetap berada pada tingkat 100% karena sejak awal seluruh peserta telah memahami pentingnya melakukan pengecekan sebelum membuka tautan yang diterima.

Hasil tersebut menunjukkan bahwa metode sosialisasi melalui presentasi, diskusi, dan tanya jawab efektif dalam meningkatkan literasi keamanan siber peserta. Meskipun sebagian besar peserta telah terbiasa menggunakan teknologi digital untuk berkomunikasi, mengakses media sosial, dan melakukan

transaksi daring, tingkat pemahaman mengenai ancaman phishing masih rendah sebelum kegiatan dilaksanakan. Kondisi ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa meningkatnya penggunaan internet turut meningkatkan risiko penyalahgunaan data pribadi, pencurian identitas, dan berbagai bentuk kejahatan siber sehingga literasi keamanan digital menjadi kebutuhan yang semakin penting [12]. Rendahnya literasi digital juga menjadi salah satu faktor yang menyebabkan masyarakat rentan terhadap berbagai modus penipuan berbasis teknologi [13].

Peningkatan hasil post-test menunjukkan bahwa edukasi yang diberikan mampu memperkuat pemahaman peserta mengenai praktik keamanan digital. Temuan ini mendukung pandangan bahwa keamanan digital merupakan serangkaian tindakan yang bertujuan melindungi informasi dan data pribadi dari berbagai ancaman di ruang siber, termasuk phishing dan penipuan daring [14]. Selain meningkatkan pengetahuan, kegiatan ini juga mendorong terbentuknya perilaku berinternet yang lebih aman, sejalan dengan konsep literasi digital yang menekankan kemampuan individu dalam mengakses, mengevaluasi, serta memanfaatkan informasi secara aman dan bertanggung jawab [15].

Selama pelaksanaan kegiatan, kendala utama yang dihadapi adalah keterbatasan waktu diskusi karena tingginya antusiasme peserta dalam berbagi pengalaman terkait penipuan digital. Kendala tersebut diatasi dengan memperpanjang sesi tanya jawab pada akhir kegiatan serta membagikan materi cetak sebagai bahan belajar mandiri. Secara keseluruhan, kegiatan berjalan dengan baik dan berhasil mencapai tujuan utama, yaitu meningkatkan pemahaman serta kesadaran Generasi Y terhadap bahaya link phishing dan pentingnya menjaga keamanan data pribadi dalam aktivitas digital sehari-hari.

4. Kesimpulan

Kegiatan edukasi keamanan siber dengan tema “Waspada Link Phishing: Cara Aman Berinternet di Era Digital” berhasil meningkatkan pengetahuan dan kesadaran peserta mengenai phishing dan keamanan data pribadi. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta pada hampir seluruh indikator yang diukur, yaitu pemahaman mengenai phishing meningkat dari 13,33% menjadi 100%, pemahaman mengenai keamanan kode OTP meningkat dari 0% menjadi 100%, serta pemahaman mengenai keamanan link meningkat dari 0% menjadi 93,33%. Peningkatan tersebut menunjukkan bahwa edukasi yang diberikan efektif dalam meningkatkan literasi digital dan kewaspadaan peserta terhadap ancaman siber pada kelompok Generasi Y. Rekomendasi bagi pengembangan program selanjutnya meliputi pelaksanaan edukasi secara berkelanjutan dengan jangkauan sasaran yang lebih luas, serta pengembangan materi melalui simulasi kasus atau praktik langsung untuk meningkatkan pemahaman peserta dalam menghadapi berbagai bentuk kejahatan siber di masa mendatang.

Daftar Pustaka

- [1] Y. Haliza, F. Handayani, and G. Gusrianda, "Urgensi literasi budaya Generasi Milenial di era digital," *Prosiding Fakultas Ushuluddin, Adab dan Dakwah*, vol. 1, no. 2, pp. 141–148, 2023.
- [2] A. M. Baqis and M. I. P. Nasution, "Pentingnya perlindungan dan keamanan data privasi di era digital," *Jurnal Manajemen dan Pendidikan Agama Islam*, vol. 3, no. 3, pp. 396–404, 2025.
- [3] F. D. Silalahi, *Keamanan Cyber (Cyber Security)*. Penerbit Yayasan Prima Agus Teknik, 2022.
- [4] H. Nugroho, M. N. Ihsan, A. Haryoko, F. Ma'arif, and F. Alifah, "Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phishing," *Alahyan: Jurnal Pengabdian Masyarakat Multidisiplin*, vol. 1, no. 2, pp. 104–111, 2023.
- [5] M. H. Wibowo and N. Fatimah, "Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime," *JoEICT (Journal of Education and Information Communication Technology)*, vol. 1, no. 1, pp. 1–5, 2017.
- [6] F. P. S. Surbakti, "Edukasi keamanan siber berdigital dengan aman," *Prima Abdika: Jurnal Pengabdian Masyarakat*, vol. 4, no. 4, pp. 868–878, 2024.

- [7] J. Manurung, A. P. E. Sihombing, and B. Pandiangan, "Sosialisasi dan edukasi tentang keamanan data dan privasi di era digital untuk meningkatkan kesadaran dan perlindungan masyarakat," *Jurnal Pengabdian Masyarakat Nauli*, vol. 2, no. 1, pp. 1–7, 2023.
- [8] K. Sussolaikah, R. D. Laksono, and A. Andria, "Pelatihan media edukasi kesadaran keamanan siber di SDN 01 Pandean Kota Madiun," *Jurnal Pengabdian Masyarakat IPTEK*, vol. 3, no. 2, pp. 131–136, 2023, doi: 10.53513/abdi.v3i2.8749.
- [9] F. Marwati and A. Astofa, "Pentingnya edukasi cyber security untuk menjaga keamanan data pribadi dari serangan cyber phishing bagi siswa/siswi PKBM Intan Tangerang Selatan," *AMMA: Jurnal Pengabdian Masyarakat*, vol. 2, no. 12, pp. 1508–1514, 2024.
- [10] E. Krisnaningsih, S. Dwiyoatno, A. D. Jubaedi, and A. Shafitri, "Increasing ethical understanding of the use of information technology through digital literacy proficiency training," *Dinamisia: Jurnal Pengabdian Kepada Masyarakat*, vol. 7, no. 3, pp. 789–801, 2023.
- [11] P. Sidiq, "Literasi digital pada masyarakat: Etis bermedia sosial, aman dan nyaman," *Jurnal Pengabdian Literasi Digital Indonesia*, vol. 3, no. 2, pp. 89–96, 2024.
- [12] D. F. Saputra, "Literasi digital untuk perlindungan data pribadi," *Jurnal Ilmu Kepolisian*, vol. 17, no. 3, 2023.
- [13] L. Panggabean, "Implementasi literasi digital dalam meningkatkan keamanan data masyarakat di era transformasi digital," *Jurnal Kemitraan kepada Masyarakat*, vol. 3, 2025.
- [14] S. Shaufiah, D. Kristinawati, R. Rochmawati, M. F. Rizal, R. Sukawati, and H. Fauziah, "Mewujudkan masyarakat desa yang cerdas digital: Edukasi etika dan keamanan digital di Pamupukan, Kuningan," *Jurnal Pengabdian Masyarakat Bangsa*, vol. 3, no. 1, pp. 27–33, 2025.
- [15] V. H. Fharaz, N. Kusnadi, and D. Rachmina, "Pengaruh literasi digital terhadap literasi e-marketing pada petani," *Jurnal Agribisnis Indonesia*, vol. 10, no. 1, pp. 169–179, 2022.