Jurnal Pengabdian Aceh, Volume 5, Nomor 3, September 2025, halaman 182–188

Sosialisasi Keamanan Siber bagi Ibu Rumah Tangga di Gampong Lambung Kota Banda Aceh

Nur Aidar, Nur Flora Arafah, Julian As'ari, Mafirah, Meutia Fadilla, Sherli Tri Lestari, Chenny Seftarita, Asri Diana, Cut Risya Varlitya

Fakultas Ekonomi dan Bisnis, Universitas Syiah Kuala, Banda Aceh, Indonesia
Email Korespondensi: nuraidar@usk.ac.id

Received: 26-06-2025	Revised: 06-08-2025	Accepted: 12-08-2025

Abstrak

Kegiatan pengabdian ini bertujuan untuk meningkatkan kesadaran dan pemahaman masyarakat terhadap bahaya kejahatan siber dan penipuan digital yang semakin marak di era teknologi informasi. Pelaksanaan kegiatan dilakukan secara tatap muka di Meunasah Gampong Lambung. Target peserta kegiatan adalah ibu rumah tangga yang bertempat tinggal di Gampong Lambung Kota Banda Aceh. Materi sosialisasi mencakup pengenalan bentuk-bentuk kejahatan siber, modus penipuan digital yang sering terjadi, serta strategi pencegahan yang dapat dilakukan oleh individu dan komunitas. Kegiatan dilengkapi dengan pemutaran video edukatif, simulasi kasus nyata, serta sesi diskusi dan tanya jawab interaktif. Hasil pengabdian menunjukkan adanya peningkatan pemahaman peserta terhadap risiko kejahatan digital dan pentingnya menjaga keamanan data pribadi. Para peserta juga memberikan tanggapan positif terhadap kegiatan ini dan menyarankan agar sosialisasi serupa dilakukan secara berkala di berbagai wilayah.

Abstract

This community service initiative was designed to enhance public awareness and comprehension of the threats posed by cybercrime and digital fraud, phenomena that have become increasingly prevalent in the contemporary information technology era. The program was implemented by a face-to-face session at Meunasah Gampong Lambung. The target participants are housewives residing in the Gampong Lambung community, Kota Banda Aceh. The educational content covered an overview of the various forms of cybercrime, common digital fraud schemes, and preventive strategies that could be adopted at both the individual and community levels. To strengthen knowledge transfer, the session was supplemented with educational video presentations, real-world case simulations, and interactive discussions, as well as question-and-answer segments. The evaluation results indicated a significant improvement in participants' understanding of digital crime risks and the critical importance of safeguarding personal data. Moreover, participants provided positive feedback on the program and recommended that similar awareness campaigns be held regularly in other communities.

Keywords: cybercrime, digital fraud, socialization, digital literacy

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi (TIK) dalam dua dekade terakhir telah menciptakan transformasi yang luar biasa dalam hampir seluruh aspek kehidupan masyarakat, mulai dari cara berinteraksi sosial, bertransaksi ekonomi, memperoleh layanan pendidikan dan kesehatan, hingga mengakses informasi yang tersedia secara luas melalui jaringan internet. Di Indonesia sendiri, adopsi teknologi digital telah mengalami pertumbuhan yang sangat signifikan, terutama setelah pandemi COVID-19 yang mendorong digitalisasi dalam berbagai sektor kehidupan, termasuk di lingkungan rumah tangga dan komunitas pedesaan. Berdasarkan laporan resmi yang diterbitkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (2020), tingkat penetrasi internet di Indonesia terus meningkat, bahkan mencapai lebih dari 70% dari total populasi, dengan penggunaan terbesar berada pada aplikasi media sosial, perpesanan instan, dan platform belanja daring.

Perkembangan teknologi informasi dan komunikasi (TIK) yang berlangsung sangat cepat dalam dua dekade terakhir telah mengubah secara fundamental pola interaksi sosial, sistem ekonomi, cara masyarakat mengakses informasi, serta mekanisme pelayanan publik di seluruh dunia, termasuk di Indonesia. Kehadiran internet yang semakin terjangkau dan penggunaan perangkat digital yang semakin masif telah membuka berbagai peluang kemudahan bagi masyarakat dalam menjalankan aktivitas sehari-hari, mulai dari komunikasi lintas wilayah, pembelajaran daring, hingga transaksi ekonomi digital yang kini menjadi bagian tidak terpisahkan dari kehidupan modern (Akbar & Wijaya, 2024). Akan tetapi, di tengah segala kemajuan dan manfaat yang ditawarkan oleh era digital ini, muncul pula berbagai tantangan baru yang kompleks dan berisiko tinggi, salah satunya adalah meningkatnya eskalasi kasus kejahatan siber (*cybercrime*) dan penipuan digital yang menyasar kelompok-kelompok masyarakat yang belum sepenuhnya memahami cara kerja sistem digital dan belum memiliki ketahanan dalam menghadapi manipulasi berbasis teknologi.

Cybercrime, yang secara luas mencakup berbagai aktivitas ilegal yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet, seperti pencurian data pribadi, peretasan akun, penyebaran *malware*, dan manipulasi psikologis melalui *phishing*, kini menjadi bentuk ancaman yang nyata dan semakin marak terjadi seiring meningkatnya aktivitas masyarakat di ruang digital. Menurut hasil tinjauan sistematis oleh Desolda (2022), keberhasilan pelaku kejahatan siber dalam menjebak korban sering kali tidak semata-mata disebabkan oleh kecanggihan teknologi yang digunakan, melainkan lebih banyak dipengaruhi oleh kelemahan dari sisi pengguna, terutama terkait kurangnya kesadaran, rendahnya literasi digital, dan kecenderungan untuk mempercayai informasi atau pesan yang tampak meyakinkan padahal berasal dari sumber yang tidak kredibel.

Di Indonesia, situasi ini diperburuk oleh fakta bahwa terdapat ketimpangan yang cukup mencolok antara masyarakat perkotaan dan pedesaan dalam hal akses terhadap pendidikan digital dan kemampuan dalam memahami serta mengelola risiko-risiko yang terkait dengan penggunaan teknologi. Penelitian oleh Afrina, Zulaikha, dan Jumila (2024) menunjukkan bahwa mayoritas penduduk desa, khususnya yang berusia dewasa dan tidak memiliki latar belakang pendidikan formal dalam bidang teknologi, cenderung hanya menjadi pengguna pasif tanpa memiliki kesadaran kritis terhadap bahaya-bahaya yang mungkin mereka hadapi di ruang digital. Bahkan, mereka kerap kali tidak menyadari bahwa informasi pribadi yang mereka unggah di media sosial atau yang mereka bagikan melalui aplikasi pesan instan dapat dimanfaatkan oleh pelaku untuk melakukan tindakan kriminal seperti pencurian identitas atau penipuan berkedok undian.

Kondisi ini menjadi semakin mengkhawatirkan ketika dikaitkan dengan kelompok ibu rumah tangga yang secara statistik memiliki waktu yang cukup lama berinteraksi dengan perangkat digital, baik untuk kegiatan sosial seperti menggunakan WhatsApp dan Facebook, maupun untuk aktivitas ekonomi seperti belanja daring dan pembayaran tagihan. Namun demikian, seperti yang disampaikan

oleh Lu, Xie, dan Zhang (2024), partisipasi perempuan, khususnya di wilayah pedesaan, dalam program literasi digital masih tergolong rendah, yang disebabkan oleh berbagai faktor mulai dari hambatan akses informasi, keterbatasan waktu, hingga rendahnya kepercayaan diri untuk mengikuti pelatihan teknologi yang dianggap terlalu teknis dan rumit.

Fenomena kerentanan kelompok ibu rumah tangga terhadap kejahatan siber diperkuat oleh temuan Jayatilaka, Arachchilage, dan Babar (2021) yang dalam studinya menunjukkan bahwa mayoritas korban *phishing* dan penipuan daring berasal dari latar belakang sosial yang tidak terbiasa mengevaluasi keabsahan pesan elektronik atau situs web yang mereka akses, sehingga mereka dengan mudah termakan oleh skema penipuan yang terstruktur secara manipulatif. Hal ini membuktikan bahwa peningkatan literasi digital bukan hanya menjadi kebutuhan, tetapi sudah menjadi keharusan untuk membentengi masyarakat dari bahaya manipulasi siber yang kian berkembang.

Mitra kegiatan pengabdian ini adalah kelompok ibu rumah tangga di Gampong Lambung, sebuah komunitas yang telah menunjukkan ketertarikan dan partisipasi dalam aktivitas digital, tetapi belum memiliki pengetahuan dasar yang memadai terkait dengan aspek keamanan dan etika dalam penggunaan teknologi. Observasi awal dan hasil diskusi informal dengan tokoh masyarakat setempat menunjukkan bahwa sebagian besar dari mereka belum pernah menerima pelatihan tentang perlindungan data pribadi, cara mengenali pesan penipuan, atau langkah-langkah yang harus dilakukan ketika menjadi korban kejahatan siber, sehingga mereka sangat membutuhkan pendampingan yang bersifat edukatif dan praktis untuk mengatasi hal tersebut.

Untuk menjawab kebutuhan ini, maka dirancanglah kegiatan pengabdian masyarakat dengan pendekatan partisipatif, di mana peserta tidak hanya menerima informasi secara pasif, tetapi dilibatkan secara aktif dalam proses belajar melalui simulasi kasus, diskusi kelompok, dan pemutaran video edukatif yang mengilustrasikan berbagai bentuk kejahatan digital secara nyata. Strategi ini sesuai dengan rekomendasi Baki dan Verma (2021), yang menyatakan bahwa efektivitas edukasi keamanan siber akan jauh lebih tinggi apabila disampaikan secara berulang, berbasis konteks lokal, dan melibatkan peran aktif peserta dalam menginternalisasi pesan yang disampaikan.

Program ini juga merupakan bentuk dukungan nyata terhadap agenda nasional dalam mendorong peningkatan literasi digital yang inklusif dan merata, sebagaimana tertuang dalam dokumen Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020–2024. Di samping itu, kegiatan ini juga mencerminkan semangat kolaboratif yang digarisbawahi oleh Atriani et al. (2024), yaitu pentingnya sinergi antara akademisi, pemerintah daerah, dan komunitas lokal dalam membangun ekosistem digital yang aman, sehat, dan adaptif terhadap tantangan masa depan. Lebih jauh, Quayyum dan Freberg (2023) menekankan bahwa keberhasilan program kesadaran keamanan digital tidak hanya terletak pada konten materinya, tetapi juga pada sejauh mana program tersebut mampu mengakomodasi kebutuhan, kapasitas, serta nilai-nilai sosial yang hidup di tengah masyarakat yang menjadi sasarannya.

Dengan demikian, kegiatan pengabdian ini dirancang tidak sekadar sebagai sarana penyuluhan, tetapi sebagai bentuk intervensi sosial yang bertujuan untuk memperkuat kapasitas masyarakat dalam menghadapi era digital yang penuh peluang sekaligus risiko. Melalui pendekatan yang holistik dan berbasis kebutuhan nyata masyarakat, diharapkan bahwa kelompok ibu rumah tangga di Gampong Lambung dapat menjadi garda terdepan dalam menyebarluaskan nilai-nilai literasi digital dan menciptakan komunitas yang lebih waspada, resilien, dan berdaya dalam menghadapi tantangan kejahatan siber di masa kini maupun yang akan datang.

METODE

Metode pelaksanaan pengabdian masyarakat ini menggunakan pendekatan partisipatif melalui sosialisasi langsung yang difokuskan pada peningkatan literasi digital dan kesadaran keamanan siber. Kegiatan dilakukan dengan metode ceramah, diskusi interaktif, pemutaran video edukatif, serta simulasi kasus kejahatan digital yang umum terjadi, seperti *phising*, rekayasa Sosial, penipuan *giveaway* atau hadiah, toko online palsu dan penipuan investasi melalui media sosial.

Kegiatan pengabdian ini dilaksanakan di Meunasah Gampong Lambung Kecamatan Meuraxa Kota Banda Aceh selama setengah hari, dengan melibatkan peserta Ibu-ibu di Gampong Lambung. Jumlah peserta yang hadir dalam kegiatan ini sebanyak 25 orang. Sebelum pelaksanaan kegiatan, tim pengabdian terlebih dahulu melakukan koordinasi dengan kepala desa untuk mengatur jadwal serta menyiapkan kebutuhan teknis seperti alat proyektor, pengeras suara.

Untuk memastikan keterlibatan aktif peserta, metode diskusi kelompok digunakan setelah sesi ceramah. Peserta dibagi dalam beberapa kelompok kecil untuk mendiskusikan studi kasus sederhana mengenai penipuan digital, kemudian mempresentasikan hasil diskusi mereka di hadapan peserta lain. Dokumentasi kegiatan dilakukan dalam bentuk foto dan video, sedangkan data hasil *pre-test* dan *post-test* dianalisis secara deskriptif untuk melihat efektivitas kegiatan sosialisasi.

HASIL DAN PEMBAHASAN

Kegiatan sosialisasi yang dilaksanakan di Gampong Lambung, dengan sasaran utama ibu rumah tangga sebagai peserta, menunjukkan keberhasilan dalam meningkatkan pemahaman masyarakat mengenai berbagai bentuk kejahatan siber dan penipuan digital yang sering terjadi dalam kehidupan sehari-hari. Pendekatan metode yang digunakan dalam kegiatan pengabdian ini, yaitu penyampaian materi secara interaktif, pemutaran video edukatif, simulasi kasus nyata, dan diskusi kelompok partisipatif, terbukti efektif dalam meningkatkan keterlibatan peserta. Studi oleh Baki dan Verma (2021) menyatakan bahwa edukasi tentang ancaman *phishing* yang bersifat kontekstual dan disampaikan dalam format yang mudah dipahami oleh masyarakat awam akan lebih mudah diinternalisasi dan diterapkan dalam kebiasaan digital sehari-hari. Hal ini terbukti dalam diskusi kelompok, di mana peserta secara aktif menceritakan pengalaman mereka menerima pesan mencurigakan dari akun tidak dikenal, dan mampu menganalisis modus penipuan tersebut setelah mendapatkan pemahaman dari sesi pelatihan.

Selain itu, ditemukan pula bahwa mayoritas peserta belum pernah menerima pelatihan, sosialisasi, ataupun penyuluhan formal mengenai literasi digital sebelumnya. Hal ini mengindikasikan masih rendahnya tingkat inklusi edukasi digital pada kelompok rentan di desa. Menurut Afrina et al. (2024), rendahnya literasi digital masyarakat Indonesia merupakan tantangan struktural yang tidak hanya disebabkan oleh minimnya akses terhadap infrastruktur digital, tetapi juga oleh kurangnya intervensi edukatif yang diarahkan secara spesifik kepada kelompok-kelompok sosial yang dianggap kurang familiar dengan teknologi digital, seperti ibu rumah tangga dan lansia.

Adapun salah satu temuan penting dari kegiatan ini adalah meningkatnya kesadaran peserta mengenai bahaya *phishing* dan manipulasi sosial (*social engineering*) setelah menyaksikan simulasi video edukatif dan berdiskusi tentang tanda-tanda umum dari pesan penipuan digital. Temuan ini memperkuat hasil studi oleh Desolda et al. (2022) yang menyimpulkan bahwa faktor manusia, seperti ketidaktahuan, rasa percaya berlebihan, serta ketidakmampuan membedakan sumber informasi yang valid, merupakan titik lemah yang paling sering dieksploitasi oleh pelaku kejahatan siber.

Dalam konteks organisasi atau komunitas, efek pendidikan ini juga menciptakan dampak berantai yang positif. Sebagian besar peserta menyatakan komitmennya untuk membagikan informasi

yang telah diperoleh kepada anggota keluarga, tetangga, dan rekan sejawat di lingkungan sekitar. Efek ini sejalan dengan fenomena *social spillover*, sebagaimana dijelaskan oleh Lu, Xie, dan Zhang (2024), di mana peningkatan literasi digital pada satu individu atau kelompok kecil dapat menyebar dan mempengaruhi lingkungan sosialnya secara lebih luas, menciptakan efek kolektif dalam membentuk kesadaran digital.

Kegiatan ini juga memberikan kontribusi pada upaya mitigasi *phishing* yang lebih strategis di tingkat komunitas. Wosah dan Win (2021) dalam tinjauan literaturnya menjelaskan bahwa program mitigasi *phishing* paling efektif ketika berbasis pada edukasi pengguna, penggunaan studi kasus lokal, dan pelatihan simulasi secara berkala. Hal yang sama diperkuat oleh Jayatilaka et al. (2021), yang menekankan bahwa pemahaman terhadap tanda-tanda manipulasi pesan digital, seperti kesalahan ejaan, tautan mencurigakan, dan tekanan waktu dalam permintaan informasi, harus diajarkan secara langsung kepada pengguna yang berisiko tinggi.

Dari sisi keberlanjutan, peserta juga menyarankan agar kegiatan serupa dapat dilakukan secara berkala dan menyasar kelompok-kelompok lain yang juga rentan terhadap penipuan digital, seperti pelajar, pedagang kecil, dan remaja. Hal ini menunjukkan bahwa masyarakat telah menyadari pentingnya edukasi berkelanjutan dan menginginkan keterlibatan yang lebih luas dalam pembangunan budaya digital yang aman. Dalam konteks ini, Lain, Kostiainen, dan Capkun (2021) menekankan pentingnya membangun sistem perlindungan kolektif dalam organisasi dan komunitas, di mana semua anggota memiliki peran dan tanggung jawab dalam menjaga keamanan digital bersama.

Dengan demikian, kegiatan pengabdian ini tidak hanya memberikan manfaat praktis dalam meningkatkan pemahaman peserta terhadap kejahatan siber, tetapi juga berhasil membangun kesadaran kolektif dan pola pikir kritis yang mendukung terbentuknya komunitas yang lebih tanggap, resilien, dan sadar akan pentingnya perlindungan terhadap data dan aktivitas digital sehari-hari. Program ini dapat menjadi model awal yang dapat direplikasi di wilayah lain dengan pendekatan yang disesuaikan secara lokal dan berbasis partisipasi masyarakat.

Sumber: Dokumentasi lapangan, 2025

Gambar 1. kegiatan sosialisasi

PENUTUP

Kegiatan pengabdian kepada masyarakat yang dilaksanakan di Gampong Lambung telah berhasil mencapai tujuannya, yaitu meningkatkan pemahaman dan kesadaran masyarakat mengenai kejahatan siber dan penipuan digital. Melalui pendekatan yang bersifat interaktif dan partisipatif, para peserta memperoleh pengetahuan praktis yang dapat diterapkan dalam kehidupan sehari-hari untuk melindungi diri dan orang-orang terdekat dari ancaman digital. Antusiasme peserta serta dukungan dari perangkat desa menunjukkan bahwa kegiatan semacam ini sangat dibutuhkan, terutama di daerah yang memiliki tingkat pemanfaatan teknologi tinggi namun belum diimbangi dengan pemahaman mengenai risiko digital. kegiatan serupa sangat disarankan untuk terus dilaksanakan secara berkala dengan jangkauan peserta yang lebih luas, tidak hanya terbatas pada kelompok ibu-ibu, tetapi juga melibatkan remaja, lansia, dan kelompok rentan lainnya. Selain itu, kolaborasi antara perguruan tinggi, pemerintah daerah, dan komunitas lokal perlu diperkuat untuk memperluas cakupan dan keberlanjutan kegiatan edukasi digital.

Sebagai penutup, pengabdian ini tidak hanya menjadi upaya pencegahan kejahatan siber secara teknis, tetapi juga merupakan bagian dari pembangunan kesadaran kolektif untuk menciptakan masyarakat digital yang aman, cerdas, dan tangguh. Dengan edukasi yang tepat dan berkelanjutan, masyarakat dapat menjadi garda terdepan dalam memerangi kejahatan digital dan membangun lingkungan digital yang sehat dan produktif.

REFERENSI

Afrina, C., Zulaikha, S. R., & Jumila. (2024). Low digital literacy in Indonesia: Online media content analysis. *Record and Library Journal, 10*(2), 374–387. https://doi.org/10.20473/rlj.V10-I2.2024.374-387

Akbar, M., & Wijaya, G. (2024). Digital literacy of rural areas in Indonesia: Challenges and opportunities. *Proceedings of RUSET 2023, International Conference on Rural Socio-Economic Transformation*. http://dx.doi.org/10.4108/eai.1-11-2023.2344347

Atriani, D., Purba, A. A., Sampetoding, E. A. M., & Husain, S. W. J. (2024). Transformation of digital literacy and cyber law in rural society: A systematic literature review. *Proceedings of RUSET 2023, International Conference on Rural Socio-Economic Transformation* http://dx.doi.org/10.4108/eai.1-11-2023.2344332

Baki, S., & Verma, R. (2021). Sixteen years of phishing user studies: What have we learned? *arXiv preprint*. https://doi.org/10.48550/arXiv.2109.04661

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys, 54*(8), 1–35. https://doi.org/10.1145/3469886

Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2021). Falling for phishing: An empirical investigation into people's email response behaviors. *arXiv preprint*. https://doi.org/10.48550/arXiv.2108.04766

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). *Pedoman literasi digital untuk masyarakat Indonesia*. Jakarta: Direktorat Jenderal Aplikasi Informatika.

Lain, D., Kostiainen, K., & Capkun, S. (2021). Phishing in organizations: Findings from a large-scale and long-term study. *arXiv preprint*. https://doi.org/10.48550/arXiv.2112.07498

Lu, Y., Xie, Q., & Zhang, Z. (2024). Digital village construction: Impact of digital literacy among rural residents. *Highlights in Business, Economics and Management, 34*, 15–21. https://doi.org/10.54097/a1n9xz43

Quayyum, F., & Freberg, G. N. (2023). Designing cybersecurity awareness solutions for the young people in rural developing countries: The need for diversity and inclusion. *arXiv preprint*. https://doi.org/10.48550/arXiv.2312.12073

Wosah, N. P., & Win, T. (2021). Phishing mitigation techniques: A literature survey. *arXiv preprint*. https://doi.org/10.5121/ijnsa.2021.13205