

Pemanfaatan Sosialisasi Digital untuk Meningkatkan Kesadaran Keamanan Jaringan di Masyarakat Desa

Utilization of Digital Socialization to Improve Network Security Awareness in Rural Communities

Fadila Nur Syifa^{1*}, Marcha Putri Ramadhanti², Amelia Nur Azizah³, Kharisma Yulia Fauzi⁴

^{1,2,3,4}Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Indonesia

Email : fadilannursyfa1805@gmail.com^{1*}, marchaprime29@gmail.com²,
amelianurazizah03@gmail.com³, kharismaayulia35@gmail.com⁴

Alamat : Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara, Kec. Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah 53127

Korespondensi penulis : fadilannursyfa1805@gmail.com

Article History:

Received: Juni 01, 2021

Revised: Juni 25, 2021

Accepted: Juli 05, 2025

Published: Juli 07, 2025

Keywords:

Public Wi-Fi, Network Security, Digital Literacy, Socialization, Cybersecurity

Abstract: *The rapid use of the internet in public spaces increases the need for free connectivity, such as public Wi-Fi. However, the low digital literacy of the community makes them vulnerable to various cyber attacks such as data theft, malware distribution, and man-in-the-middle attacks. This study aims to analyze the effectiveness of socialization activities as a means of increasing awareness of network security in rural communities. The activities were carried out in Darmakradenan Village, Grumbul Karangpucung using a participatory method based on direct education. The results showed an increase in public understanding of public network threats and preventive measures such as the use of VPNs and network security verification. This study shows that community-based socialization is effective in building a safe and wise digital culture at the local level.*

Abstrak

Pesatnya penggunaan internet di ruang publik meningkatkan kebutuhan akan konektivitas gratis, seperti Wi-Fi publik. Namun, rendahnya literasi digital masyarakat membuat mereka rentan terhadap berbagai serangan siber seperti pencurian data, penyebaran malware, dan serangan *man-in-the-middle*. Penelitian ini bertujuan untuk menganalisis efektivitas kegiatan sosialisasi sebagai sarana peningkatan kesadaran keamanan jaringan pada masyarakat desa. Kegiatan dilakukan di Desa Darmakradenan Grumbul Karangpucung dengan metode partisipatif berbasis edukasi langsung. Hasil menunjukkan adanya peningkatan pemahaman masyarakat mengenai ancaman jaringan publik serta tindakan preventif seperti penggunaan VPN dan verifikasi keamanan jaringan. Penelitian ini menunjukkan bahwa sosialisasi berbasis komunitas efektif dalam membangun budaya digital yang aman dan bijak di tingkat lokal.

Kata kunci: Wi-Fi Publik, Keamanan Jaringan, Literasi Digital, Sosialisasi, Keamanan Siber

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Dalam dua dekade terakhir, internet telah menjadi infrastruktur utama dalam menunjang aktivitas ekonomi, sosial, pendidikan, hingga pemerintahan. Digitalisasi proses kerja dan interaksi sosial semakin intensif seiring dengan meningkatnya penetrasi perangkat mobile dan akses internet global. Tidak hanya di perkotaan, tren ini juga merambah ke daerah pedesaan, menciptakan ketergantungan baru terhadap

konektivitas digital (Kemp, 2023).

Salah satu bentuk koneksi internet yang paling mudah dijangkau oleh masyarakat adalah melalui jaringan Wi-Fi publik. Wi-Fi publik biasanya tersedia secara gratis di berbagai ruang publik seperti kafe, pusat perbelanjaan, stasiun, hingga taman kota. Keberadaannya memberikan kemudahan luar biasa bagi pengguna untuk tetap terhubung dengan dunia digital tanpa harus mengandalkan kuota data pribadi. Namun, di balik kenyamanan tersebut, Wi-Fi publik menyimpan berbagai potensi ancaman keamanan yang serius (Gupta et al., 2023).

Banyak pengguna tidak menyadari bahwa Wi-Fi publik memiliki tingkat keamanan yang rendah. Beberapa jenis serangan siber umum yang dapat terjadi melalui jaringan ini antara lain: pencurian data pribadi, serangan *man-in-the-middle* (MitM), pengintaian (*sniffing*), hingga eksploitasi melalui jaringan Wi-Fi palsu atau *rogue hotspot* (Bheevgade, et al., 2024). Serangan-serangan tersebut memungkinkan pihak tidak bertanggung jawab untuk mengakses informasi sensitif seperti kredensial login, data perbankan, hingga file pribadi milik pengguna tanpa sepengetahuan mereka.

Rendahnya literasi digital, khususnya dalam aspek keamanan siber, menjadi salah satu faktor utama yang memperparah risiko tersebut. Menurut penelitian Rajan Gupta et al. (2023), masih banyak pengguna internet terutama dari kelompok masyarakat umum yang belum memahami cara kerja ancaman digital dan bagaimana melindungi diri dari serangan melalui jaringan terbuka. Padahal, seiring meningkatnya insiden kejahatan siber di Indonesia, membangun kesadaran dan pemahaman masyarakat terhadap pentingnya keamanan jaringan menjadi hal yang sangat mendesak.

Untuk menjawab tantangan tersebut, dibutuhkan intervensi berbasis edukasi yang dapat menjangkau masyarakat secara langsung. Edukasi ini tidak hanya menitikberatkan pada pengetahuan teknis, tetapi juga membentuk kebiasaan dan pola pikir yang lebih waspada terhadap risiko digital. Salah satu strategi yang potensial adalah melalui kegiatan sosialisasi komunitas yang dilakukan secara partisipatif dan kontekstual, sesuai dengan kebutuhan dan kondisi masyarakat setempat (Livingstone & Helsper, 2007).

Penelitian ini dilakukan untuk mengkaji efektivitas kegiatan sosialisasi dengan tema “Jangan Sembarangan Connect ke Wi-Fi” sebagai upaya membangun kesadaran keamanan digital di lingkungan masyarakat desa. Sosialisasi ini tidak hanya menyampaikan informasi mengenai bahaya penggunaan Wi-Fi publik tanpa pengamanan, tetapi juga memberikan solusi praktis yang dapat diterapkan sehari-hari. Fokus penelitian diarahkan pada pemahaman dan perubahan sikap peserta terhadap kebiasaan penggunaan jaringan publik, khususnya di kalangan pemuda Karang Taruna Desa Darmakradenan, Kecamatan Ajibarang.

2. METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode partisipatif edukatif. Pendekatan ini dipilih untuk memungkinkan pemahaman yang mendalam terhadap fenomena yang diteliti, yaitu tingkat kesadaran masyarakat terhadap keamanan jaringan Wi-Fi publik serta bagaimana perubahan pengetahuan dan sikap dapat terjadi melalui intervensi edukatif yang bersifat langsung dan kontekstual (Creswell, 2014; Stringer, 2014).

Penelitian dilaksanakan pada tanggal 18 April 2025 di Desa Darmakradenan Grumbul Karangpucung, Kecamatan Ajibarang, Kabupaten Banyumas. Subjek dalam kegiatan ini adalah anggota Karang Taruna setempat sebanyak 15 orang yang dipilih secara purposif berdasarkan pertimbangan keterlibatan aktif mereka dalam penggunaan internet, khususnya jaringan Wi-Fi publik di lingkungan sekitar.

Penelitian ini bersifat partisipatif karena melibatkan subjek sebagai mitra aktif dalam proses edukasi, tidak hanya sebagai objek penerima informasi. Model ini mendekati prinsip *community-based learning*, di mana peserta bukan hanya mendengarkan, tetapi turut aktif berdiskusi dan merefleksikan pengalaman mereka terkait keamanan digital (Bequette & Bequette, 2012).

Tahapan pelaksanaan kegiatan dibagi ke dalam lima langkah utama, yaitu:

1. Identifikasi Sasaran Sosialisasi

Langkah awal adalah mengidentifikasi karakteristik peserta yang sesuai dengan fokus penelitian. Dalam hal ini, sasaran adalah masyarakat muda (remaja dan dewasa awal) yang sering mengakses jaringan Wi-Fi publik di area publik seperti kafe, sekolah, pusat perbelanjaan, dan fasilitas umum lainnya. Identifikasi dilakukan melalui pengamatan awal dan komunikasi dengan pengurus Karang Taruna.

2. Penyusunan Materi Sosialisasi

Materi sosialisasi disusun berdasarkan studi literatur terkait ancaman siber yang umum terjadi pada jaringan Wi-Fi publik. Materi difokuskan pada:

- a. Definisi dan karakteristik Wi-Fi publik
- b. Ancaman siber seperti *man-in-the-middle attack*, *rogue hotspot*, dan sniffing
- c. Dampak pencurian data pribadi
- d. Tips praktis perlindungan data, seperti penggunaan VPN, pengelolaan kata sandi, dan langkah verifikasi jaringan

Materi dirancang secara ringkas, relevan, dan komunikatif agar mudah dipahami oleh peserta dengan latar belakang non-teknis.

3. Pemilihan Media dan Metode Penyampaian

Untuk menunjang penyampaian materi yang efektif, digunakan media visual berupa presentasi PowerPoint, infografik, serta pendekatan diskusi interaktif. Model penyampaian bersifat dua arah, sehingga peserta didorong untuk mengajukan pertanyaan, berbagi pengalaman pribadi, serta memberikan respons terhadap materi yang diberikan.

4. Pelaksanaan Sosialisasi

Kegiatan dilaksanakan secara tatap muka di balai desa. Kegiatan dimulai dengan pembukaan dan pengantar mengenai pentingnya keamanan digital, dilanjutkan dengan pemaparan materi oleh tim peneliti, serta sesi diskusi kelompok dan tanya jawab. Situasi informal sengaja dibangun agar peserta merasa nyaman untuk terlibat aktif dalam diskusi dan mengungkapkan pendapat.

5. Evaluasi dan Pengumpulan Data

Setelah kegiatan sosialisasi selesai, dilakukan evaluasi untuk mengetahui seberapa besar pemahaman dan dampak dari kegiatan. Evaluasi dilakukan melalui:

- a. Wawancara semi-terstruktur terhadap beberapa peserta secara acak untuk menggali perubahan persepsi dan pemahaman
- b. Observasi langsung selama diskusi berlangsung, untuk melihat partisipasi dan respons peserta terhadap materi
- c. Catatan lapangan, yang digunakan untuk mencatat dinamika kegiatan serta komentar-komentar penting dari peserta

Data dari hasil observasi dan wawancara dianalisis secara deskriptif dengan cara mereduksi informasi menjadi tema-tema pokok yang berkaitan dengan tingkat pemahaman, perubahan sikap, serta rekomendasi dari peserta.

Dengan metode ini, penelitian diharapkan mampu menghasilkan gambaran nyata mengenai efektivitas pendekatan edukatif dalam meningkatkan literasi keamanan jaringan di masyarakat desa.

3. HASIL

Kegiatan sosialisasi bertema “*Jangan Sembarangan Connect ke Wi-Fi*” dilaksanakan dengan lancar dan sesuai dengan rencana. Peserta yang hadir terdiri dari 15 orang anggota Karang Taruna Desa Darmakradenan, yang sebagian besar merupakan pemuda usia produktif dengan tingkat penggunaan internet yang tinggi dalam kehidupan sehari-hari.

Materi sosialisasi disusun untuk menyentuh aspek fundamental keamanan jaringan,

khususnya yang berkaitan dengan penggunaan Wi-Fi publik. Topik yang disampaikan meliputi:

1. Bahaya Wi-Fi publik tanpa pengamanan, termasuk potensi akses ilegal terhadap data pribadi.
2. Jenis-jenis serangan siber, seperti *man-in-the-middle attack*, *rogue hotspot*, dan *packet sniffing*, yang dapat terjadi ketika perangkat pengguna terkoneksi ke jaringan publik yang tidak aman.
3. Solusi pencegahan, seperti penggunaan Virtual Private Network (VPN), memverifikasi nama jaringan sebelum terkoneksi, serta menghindari menyimpan informasi penting (misalnya kata sandi dan data perbankan) saat menggunakan Wi-Fi publik.

Partisipasi dan Respons Peserta

Selama kegiatan berlangsung, peserta menunjukkan antusiasme dan keterlibatan yang tinggi. Diskusi interaktif berjalan aktif, ditandai dengan banyaknya pertanyaan yang diajukan terkait praktik penggunaan internet sehari-hari. Hal ini menunjukkan bahwa meskipun pemahaman awal tentang ancaman digital masih minim, terdapat keingintahuan yang tinggi untuk belajar dan memahami isu tersebut lebih dalam.

Temuan dari Evaluasi Kualitatif

Evaluasi dilakukan melalui wawancara semi-terstruktur terhadap beberapa peserta setelah kegiatan. Temuan utama dari evaluasi ini meliputi:

1. Rendahnya pengetahuan awal
Mayoritas peserta mengaku tidak mengetahui bahwa Wi-Fi publik dapat menjadi jalur masuk bagi pelaku kejahatan siber. Sebagian besar peserta terbiasa langsung terhubung ke jaringan publik tanpa pertimbangan keamanan apa pun.
2. Peningkatan kesadaran setelah sosialisasi
Setelah menerima pemaparan materi, peserta menunjukkan pemahaman baru tentang pentingnya menjaga keamanan data pribadi saat online. Mereka mulai mengenali ancaman yang sebelumnya dianggap tidak signifikan, seperti jaringan Wi-Fi palsu yang dibuat menyerupai jaringan resmi.
3. Perubahan sikap dan niat berperilaku aman
Beberapa peserta menyatakan akan mulai menerapkan langkah-langkah pencegahan, seperti menghindari koneksi otomatis ke jaringan publik, menggunakan VPN, serta tidak melakukan transaksi penting saat menggunakan Wi-Fi gratis.

Temuan ini mengindikasikan bahwa edukasi langsung berbasis komunitas memiliki dampak signifikan dalam membentuk kesadaran dan sikap baru terkait keamanan digital. Perubahan ini tidak hanya bersifat kognitif (pemahaman), tetapi juga afektif (sikap) dan potensial menuju perubahan perilaku digital yang lebih aman (Nutbeam, 2000).

Analisis dan Interpretasi

Dari perspektif literasi digital, peningkatan pemahaman peserta pasca-sosialisasi mencerminkan keberhasilan transfer pengetahuan yang relevan dengan konteks kehidupan mereka. Temuan ini sejalan dengan penelitian oleh Rajan Gupta et al. (2023) yang menekankan bahwa pendekatan edukatif berbasis komunitas merupakan salah satu strategi efektif dalam menurunkan risiko kejahatan siber di kalangan masyarakat umum.

Selain itu, pendekatan partisipatif yang digunakan dalam kegiatan ini mampu membangun rasa kepemilikan peserta terhadap masalah yang dihadapi. Diskusi yang terbuka dan reflektif menciptakan ruang aman bagi peserta untuk mengakui kesalahan digital yang umum dilakukan, sekaligus membuka peluang untuk belajar dari pengalaman satu sama lain.

Dengan melihat hasil ini, dapat disimpulkan bahwa sosialisasi tidak hanya berfungsi sebagai sarana penyebaran informasi, tetapi juga sebagai alat transformasi sosial yang memungkinkan masyarakat beradaptasi dengan tantangan dunia digital secara lebih bijak dan bertanggung jawab.

4. KESIMPULAN

Kegiatan sosialisasi bertema “*Jangan Sembarangan Connect ke Wi-Fi*” terbukti efektif dalam meningkatkan kesadaran dan pemahaman masyarakat terhadap pentingnya keamanan jaringan, khususnya dalam penggunaan Wi-Fi publik. Edukasi yang disampaikan melalui pendekatan partisipatif dengan kombinasi presentasi visual dan diskusi interaktif berhasil mendorong keterlibatan aktif peserta, serta membentuk pemahaman yang lebih baik terhadap berbagai ancaman siber seperti *man-in-the-middle*, *rogue hotspot*, dan pencurian data. Perubahan sikap peserta tercermin dari meningkatnya kehati-hatian dalam mengakses jaringan publik serta munculnya kesadaran terhadap pentingnya penggunaan alat proteksi seperti VPN.

Temuan ini menunjukkan bahwa pendekatan edukasi berbasis komunitas dapat menjadi strategi efektif dalam membentuk budaya digital yang aman dan bertanggung jawab, terutama di tingkat akar rumput. Sosialisasi semacam ini berperan penting dalam menjembatani kesenjangan literasi digital, khususnya bagi masyarakat yang belum tersentuh edukasi formal tentang keamanan siber. Oleh karena itu, model kegiatan ini direkomendasikan untuk

direplikasi secara luas di berbagai komunitas lokal guna menciptakan ekosistem digital yang lebih tangguh terhadap ancaman keamanan informasi di era keterhubungan yang semakin kompleks.

DAFTAR REFERENSI

- Bequette, M. B., & Bequette, J. W. (2012). Community-based learning: The future of education and research. *Journal of Community Engagement and Scholarship*, 5(1), 32–44.
- Bheevgade, P., Saha, C., Nath, R., Dabhade, S., Barot, H., & Junare, S. O. (2024). The rise of public Wi-Fi and threats. In *Lecture Notes in Electrical Engineering* (Vol. 1075, pp. 175–189). Springer. https://doi.org/10.1007/978-981-99-5091-1_13
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Gupta, R., et al. (2023). The dangers of public Wi-Fi: How to protect your device through cyber security. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 3016–3022. <https://doi.org/10.17762/ijritcc.v11i9.9409>
- Kemp, S. (2023). *Digital 2023: Global overview report*. DataReportal. <https://datareportal.com/reports/digital-2023-global-overview-report>
- Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671–696. <https://doi.org/10.1177/1461444807080335>
- Nutbeam, D. (2000). Health literacy as a public health goal: A challenge for contemporary health education and communication strategies into the 21st century. *Health Promotion International*, 15(3), 259–267. <https://doi.org/10.1093/heapro/15.3.259>
- Stringer, E. T. (2014). *Action research* (4th ed.). SAGE Publications.