KAMPUS AKADEMIK PUBLISING
Jurnal Akademik Pengabdian Masyarakat (JAPM)
Vol.4, No.3 Mei 2026
e-ISSN: 3030-8631, p-ISSN : 3030-864X, Hal 314-320
DOI : https://doi.org/10.61722/japm.v4i3.9841

Sosialisasi Keamanan Jaringan: Bahaya Sniffing Pada Wifi Umum Terhadap Masyarakat

Jhazkia Putri Rizan, Marisha Setiyani, Kurnia Safitri, Nabila Putri Rahmalia, Ito Setiawan
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Purwokerto, Jawa Tengah, Indonesia, 53161
*Penulis Korespondensi: putririzann@gmail.com, nabilaask963@gmail.com, sharisha076@gmail.com, niaasftr2116@gmail.com

Abstract. *The rapid growth of information technology has made people use the internet in many daily activities, such as communication, education, and financial transactions like mobile banking. However, using public Wi-Fi without proper security can be risky, especially due to threats like sniffing, where attackers can intercept and access users' data without their knowledge. This outreach activity aims to increase public awareness about the dangers of sniffing and the importance of safe internet use. The method used was a descriptive approach, including material presentation, interactive discussions, question-and-answer sessions, and questionnaires. The activity was conducted with members of the Dawis group in RT 09/RW 07, Kranji Village, East Purwokerto. The results showed that all participants (100%) understood the material, with 62.5% agreeing and 37.5% strongly agreeing that it was easy to understand and relevant to their daily lives. Participants also became more aware of the risks of public Wi-Fi and learned simple ways to stay safe, such as avoiding access to important accounts, using HTTPS, and enabling two-factor authentication. In conclusion, this activity successfully improved digital security awareness and encouraged safer and more responsible internet use.*

Keywords: network security; sniffing; public Wi-Fi; digital literacy; data security

Abstrak. Perkembangan teknologi informasi yang pesat mendorong masyarakat untuk memanfaatkan internet dalam berbagai aktivitas, seperti komunikasi, pendidikan, dan transaksi keuangan melalui layanan digital seperti mobile banking. Namun, penggunaan Wi-Fi publik tanpa keamanan yang memadai memiliki risiko, salah satunya adalah ancaman sniffing, yaitu penyadapan data oleh pihak yang tidak bertanggung jawab tanpa sepengetahuan pengguna. Kegiatan sosialisasi ini bertujuan untuk meningkatkan pemahaman masyarakat mengenai bahaya sniffing serta pentingnya penggunaan internet yang aman. Metode yang digunakan adalah pendekatan deskriptif melalui penyampaian materi, diskusi interaktif, sesi tanya jawab, dan pengisian kuesioner. Kegiatan dilaksanakan kepada ibu-ibu Dawis RT 09/RW 07 Kelurahan Kranji, Purwokerto Timur. Hasil kegiatan menunjukkan bahwa seluruh peserta (100%) memahami materi yang disampaikan, dengan 62,5% menyatakan setuju dan 37,5% sangat setuju bahwa materi mudah dipahami dan relevan dengan kehidupan sehari-hari. Selain itu, peserta menjadi lebih sadar terhadap risiko penggunaan Wi-Fi publik serta memahami langkah-langkah pencegahan, seperti menghindari akses akun penting, menggunakan HTTPS, dan mengaktifkan autentikasi dua faktor. Dengan demikian, kegiatan ini berhasil meningkatkan literasi keamanan digital serta mendorong perilaku penggunaan internet yang lebih aman dan bijak.

Kata kunci: keamanan jaringan*; sniffing; Wi-Fi publik; literasi digital; keamanan data*

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah memberikan berbagai kemudahan bagi masyarakat dalam menjalankan aktivitas sehari-hari. Internet kini tidak hanya digunakan sebagai sarana komunikasi dan hiburan, tetapi juga dimanfaatkan dalam

Naskah Masuk: 01 April 2026; Revisi: 10 April 2026; Diterima: 02 Mei 2026; ; Terbit: 02 Mei 2026

bidang pendidikan, bisnis, serta transaksi keuangan melalui layanan digital seperti mobile banking (m-banking). Kehadiran layanan digital tersebut memungkinkan masyarakat melakukan berbagai aktivitas secara lebih cepat, mudah, dan efisien tanpa harus datang langsung ke tempat layanan.

Namun, di balik kemudahan tersebut, perkembangan teknologi juga menghadirkan tantangan baru berupa meningkatnya ancaman kejahatan siber yang dapat membahayakan keamanan data pribadi pengguna. Salah satu ancaman yang sering terjadi adalah penggunaan jaringan internet yang tidak aman, khususnya Wi-Fi publik. Wi-Fi publik banyak digunakan masyarakat karena mudah diakses dan tersedia secara gratis di berbagai tempat umum.

Salah satu bentuk ancaman pada jaringan Wi-Fi publik adalah sniffing, yaitu tindakan penyadapan data yang dikirimkan melalui jaringan internet tanpa sepengetahuan pengguna. Risiko ini menjadi semakin berbahaya apabila pengguna mengakses layanan penting seperti m-banking melalui jaringan yang tidak aman. Oleh karena itu, edukasi mengenai keamanan digital menjadi sangat penting untuk meningkatkan kesadaran masyarakat.

Berdasarkan kondisi tersebut, kegiatan sosialisasi keamanan digital dilaksanakan kepada ibu-ibu Dawis RT 09/RW 07 Kelurahan Kranji sebagai upaya meningkatkan literasi masyarakat terkait keamanan penggunaan internet. Penelitian ini bertujuan untuk meningkatkan pemahaman masyarakat terhadap bahaya sniffing serta mendorong penggunaan internet yang lebih aman.

2. KAJIAN TEORITIS

Sniffing atau packet sniffing merupakan teknik pemantauan lalu lintas data pada jaringan komputer dengan cara menangkap dan menganalisis paket data yang dikirim antarperangkat dalam suatu jaringan. Menurut Pranata, Abdillah, dan Ependi (2015), sniffing adalah proses monitoring terhadap setiap paket data yang melintas di jaringan. Melalui teknik ini, pelaku dapat menangkap informasi penting seperti username, password, dan data sensitif lainnya apabila data tersebut tidak terlindungi dengan sistem keamanan yang memadai.

Dalam perkembangan teknologi jaringan saat ini, sniffing menjadi salah satu ancaman utama pada jaringan publik, terutama Wi-Fi umum. Penelitian Anwar (2024) menjelaskan bahwa serangan packet sniffing pada jaringan Wi-Fi dapat dimanfaatkan untuk menangkap data pengguna melalui kelemahan protokol jaringan dan kurangnya enkripsi. Hal ini berpotensi menyebabkan pencurian informasi pribadi maupun finansial pengguna yang terhubung pada jaringan tersebut.

Selain itu, jaringan publik yang masih menggunakan protokol HTTP memiliki risiko lebih tinggi terhadap pencurian sesi login (session hijacking). Studi oleh Hasan dkk. (2025) menunjukkan bahwa pada jaringan publik dengan teknik sniffing, pelaku dapat mengambil akses akun tanpa perlu mengetahui kata sandi secara langsung, yang sangat berbahaya bagi pengguna layanan transaksi keuangan.

Risiko ini diperburuk oleh rendahnya tingkat pengungkapan keamanan siber pada sektor-sektor krusial seperti perbankan. Oleh karena itu, langkah-langkah pencegahan seperti penggunaan HTTPS/SSL, VPN, serta menghindari akses data sensitif melalui Wi-Fi publik menjadi sangat penting untuk meminimalkan risiko kejahatan siber.

3. METODE PENELITIAN

Kegiatan sosialisasi ini menggunakan pendekatan deskriptif yang bertujuan untuk memberikan pemahaman kepada masyarakat mengenai bahaya sniffing pada penggunaan Wi-Fi umum. Pelaksanaan kegiatan dilakukan melalui penyampaian materi, diskusi interaktif, sesi tanya jawab, serta pengisian kuesioner evaluasi.

Materi yang diberikan mencakup pengertian sniffing, dampaknya, serta langkah pencegahan seperti menghindari login akun penting di Wi-Fi umum, menggunakan HTTPS, dan mengaktifkan verifikasi tambahan. Data diperoleh melalui observasi dan respons peserta selama kegiatan berlangsung, kemudian dianalisis secara deskriptif.

4. HASIL DAN PEMBAHASAN

Hasil kegiatan sosialisasi menunjukkan bahwa tingkat pemahaman Ibu-Ibu Dawis RT 09/RW 07 Kelurahan Kranji, Purwokerto Timur terhadap materi bahaya sniffing pada penggunaan Wi-Fi publik mengalami peningkatan yang signifikan. Berdasarkan data yang diperoleh dari 16 responden, seluruh peserta (100%) menyatakan telah memahami

materi yang disampaikan. Sebanyak 10 responden (62,5%) menyatakan setuju dan 6 responden (37,5%) menyatakan sangat setuju bahwa materi yang diberikan mudah dipahami serta relevan dengan kehidupan sehari-hari.

Selama kegiatan berlangsung, peserta menunjukkan peningkatan pemahaman terkait risiko penggunaan Wi-Fi publik, khususnya potensi pencurian data melalui teknik sniffing. Peserta mulai memahami bahwa aktivitas seperti login akun media sosial, email, hingga transaksi digital melalui jaringan publik yang tidak aman dapat menyebabkan kebocoran data pribadi, seperti username, password, dan informasi sensitif lainnya.

A. Tingkat Pemahaman Masyarakat terhadap Bahaya Sniffing

Hasil penelitian menunjukkan bahwa seluruh peserta mampu memahami materi yang disampaikan dengan baik. Hal ini mengindikasikan bahwa metode sosialisasi yang digunakan, seperti penyampaian materi secara langsung, diskusi interaktif, serta sesi tanya jawab, efektif dalam meningkatkan literasi digital masyarakat.

Jika dikaitkan dengan teori keamanan jaringan, kondisi ini menunjukkan bahwa ancaman sniffing pada Wi-Fi publik menjadi lebih berbahaya bukan hanya karena faktor teknis, tetapi juga karena rendahnya pemahaman pengguna terhadap risiko yang ada. Sebelum sosialisasi, sebagian besar peserta masih menganggap Wi-Fi publik sebagai fasilitas yang aman digunakan tanpa mempertimbangkan aspek keamanan data.

B. Dampak Sniffing terhadap Keamanan Data Pengguna

Sniffing memiliki dampak yang signifikan terhadap keamanan data pengguna, terutama pada jaringan Wi-Fi publik yang tidak memiliki sistem enkripsi yang memadai. Data yang dikirim melalui protokol yang tidak aman, seperti HTTP, dapat dengan mudah disadap oleh pihak yang tidak bertanggung jawab.

Dampak utama dari serangan sniffing meliputi:

- Kebocoran data pribadi (username, password, email)
- Pembajakan akun (account hijacking)
- Pencurian data keuangan (mobile banking)
- Hilangnya privasi digital pengguna

Selain itu, sniffing juga dapat menjadi pintu masuk bagi serangan lanjutan seperti *man-in-the-middle attack* dan *session hijacking*, yang memungkinkan pelaku mengambil alih akses akun pengguna tanpa diketahui.

C. Analisis Peningkatan Literasi Digital Masyarakat

Secara keseluruhan, hasil kegiatan menunjukkan adanya peningkatan pemahaman Ibu-Ibu Dawis RT 09/RW 07 Kelurahan Kranji, Purwokerto Timur setelah mengikuti sosialisasi. Hal ini mengindikasikan bahwa sebelumnya terdapat keterbatasan pengetahuan terkait keamanan digital, khususnya dalam penggunaan Wi-Fi publik. Tingginya tingkat pemahaman (100%) setelah sosialisasi menunjukkan bahwa masyarakat sebenarnya mampu memahami konsep keamanan digital apabila disampaikan dengan pendekatan yang sederhana dan kontekstual.

Namun demikian, peningkatan pemahaman tidak selalu diikuti dengan perubahan perilaku. Dalam praktiknya, pengguna masih berpotensi menggunakan Wi-Fi publik secara tidak aman karena faktor kenyamanan, kemudahan akses, dan kebiasaan. Hal ini menunjukkan bahwa masalah keamanan digital tidak hanya terletak pada aspek teknologi, tetapi juga pada perilaku pengguna (*human factor*).

Oleh karena itu, edukasi keamanan digital perlu dilakukan secara berkelanjutan dan tidak hanya bersifat satu kali kegiatan. Pendekatan yang lebih aplikatif, seperti simulasi kasus atau praktik langsung, dapat meningkatkan kemungkinan perubahan perilaku pengguna dalam menggunakan internet secara aman.

D. Implikasi Hasil Kegiatan

Kegiatan sosialisasi ini memberikan dampak positif dalam meningkatkan kesadaran masyarakat terhadap pentingnya keamanan digital. Secara praktis, kegiatan ini dapat menjadi salah satu bentuk upaya preventif dalam mengurangi risiko kejahatan siber, khususnya yang berkaitan dengan penggunaan Wi-Fi publik.

Penggunaan teknologi tambahan seperti Virtual Private Network (VPN) juga dapat menjadi salah satu solusi dalam meningkatkan keamanan saat mengakses jaringan publik. Namun, untuk mencapai hasil yang lebih optimal, kegiatan serupa perlu dilakukan secara berkelanjutan dengan pendekatan yang lebih aplikatif, seperti simulasi atau praktik langsung.

5. KESIMPULAN DAN SARAN

Kegiatan sosialisasi mengenai bahaya sniffing pada penggunaan Wi-Fi publik berhasil meningkatkan pemahaman masyarakat terhadap risiko keamanan digital, khususnya dalam penggunaan jaringan internet yang tidak aman. Hal ini ditunjukkan dari hasil evaluasi di mana seluruh peserta mampu memahami materi yang disampaikan, sehingga tujuan penelitian untuk meningkatkan kesadaran dan pengetahuan masyarakat mengenai ancaman sniffing dapat tercapai. Temuan ini menunjukkan bahwa metode sosialisasi melalui penyampaian materi, diskusi interaktif, dan evaluasi kuesioner efektif dalam meningkatkan literasi digital masyarakat. Meskipun demikian, penelitian ini memiliki keterbatasan pada jumlah peserta yang terbatas serta cakupan kegiatan yang hanya dilakukan pada satu kelompok masyarakat, sehingga hasilnya belum dapat digeneralisasikan secara luas. Oleh karena itu, disarankan agar kegiatan serupa dilakukan secara berkelanjutan dengan cakupan peserta yang lebih luas dan materi yang lebih mendalam, serta dikembangkan dengan metode tambahan seperti simulasi praktik agar pemahaman masyarakat terhadap keamanan digital dapat semakin optimal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam pelaksanaan kegiatan sosialisasi ini. Ucapan terima kasih disampaikan kepada dosen pengampu mata kuliah Jaringan Komputer yang telah memberikan arahan dan bimbingan selama proses penyusunan karya ilmiah ini.

Selain itu, penulis juga mengucapkan terima kasih kepada ibu-ibu Dawis RT 09/RW 07 Kelurahan Kranji yang telah bersedia menjadi peserta dalam kegiatan sosialisasi serta berpartisipasi aktif selama kegiatan berlangsung.

Penulis juga menyampaikan apresiasi kepada seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, sehingga kegiatan dan penyusunan jurnal ini dapat berjalan dengan baik.

DAFTAR REFERENSI

Anwar, A. N. (2024). Network security analysis on the internet facility (Wi-Fi) UIN Syarif Hidayatullah Jakarta against packet sniffing attacks. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4(3), 771–776.

Arini, A., Arsalan, M. L., & Sukmana, H. T. (2024). Keamanan jaringan Wi-Fi terhadap serangan packet sniffing menggunakan firewall rule (Studi kasus: PT Akurat.co). Cyber Security dan Forensik Digital, 6(2), 30–38.

Hasan, T. M., Albar, R., TB, D. R. Y., & Wibawa, M. B. (2025). Analisis risiko keamanan WiFi.id manage service (WMS) pada jaringan publik dengan teknik sniffing. Journal of Informatics and Computer Science, 11(2), 66–74.

Pranata, H., Abdillah, L. A., & Ependi, U. (2015). Analisis keamanan protokol Secure Socket Layer (SSL) terhadap proses sniffing di jaringan. ArXiv Preprint ArXiv:1508.05457.

Rahman, F., Hidayat, T., & Nugroho, A. (2023). Analisis serangan sniffing terhadap keamanan data pengguna jaringan publik. Jurnal Teknologi Informasi dan Komunikasi, 8(2), 112–120.

Kurniawan, A., & Saputra, R. (2023). Analisis keamanan jaringan wireless terhadap serangan cyber. Jurnal Informatika dan Komputer, 9(3), 201–210.

Hidayat, M., & Prasetyo, E. (2021). Evaluasi keamanan jaringan berbasis Wi-Fi pada lingkungan publik. Jurnal Teknologi Informasi, 7(1), 15–23.

Saputri, R., & Andika, M. (2024). Analisis literasi keamanan digital masyarakat terhadap penggunaan internet. Jurnal Ilmu Komputer dan Informasi, 12(2), 99–108.

Fauzan, M., & Hakim, L. (2023). Studi keamanan jaringan terhadap serangan man-in-the-middle. Jurnal Cyber Security Indonesia, 4(1), 23–31.

Wijaya, H., & Gunawan, B. (2022). Penerapan VPN dalam meningkatkan keamanan jaringan publik. Jurnal Teknologi Digital, 6(2), 134–142.