Jurnal Penelitian Nusantara
Volume 1 ; Nomor 12 ; Desember 2025 ; Page 643-649
Doi : https://doi.org/10.59435/menulis.v1i12.835
Website : https://padangjurnal.web.id/index.php/menulis
E-ISSN : 3088-988X

Pengenalan Ancaman Dan Pencegahan Serangan Siber Melalui Edukasi Keamanan Jaringan Wi-Fi Dan Internet

Dewi Agustina[1], Maila Rizqi Aulia[2], Naufal Afriandi[3]

[1] Sistem Informasi, Sains dan Teknologi, UIN Sulthan Thaha Saifuddin Jambi
[2] Sistem Informasi, Sains dan Teknologi, UIN Sulthan Thaha Saifuddin Jambi
[3] Sistem Informasi, Sains dan Teknologi, UIN Sulthan Thaha Saifuddin Jambi
[1]dewiagustina1504@gmail.com, [2]mailarizqiaulia019@gmail.com, [3]nopal3392@gmail.com

Abstrak

Perkembangan teknologi digital mendorong meningkatnya penggunaan jaringan Wi-Fi dan internet di lingkungan akademik. Namun, tingginya intensitas penggunaan tersebut juga diiringi dengan meningkatnya risiko ancaman keamanan siber, terutama bagi pengguna yang belum memiliki pemahaman keamanan jaringan yang memadai. Kegiatan sosialisasi ini bertujuan untuk meningkatkan pemahaman dan kesadaran mahasiswa terhadap ancaman serta upaya pencegahan serangan siber pada jaringan Wi-Fi dan internet. Sosialisasi dilaksanakan melalui penyampaian materi secara langsung yang disertai sesi diskusi dan tanya jawab kepada 20 mahasiswa Program Studi Pendidikan Agama Islam (PAI) UIN Sulthan Thaha Saifuddin Jambi. Hasil kegiatan menunjukkan bahwa peserta mampu mengenali berbagai jenis ancaman siber, seperti *eavesdropping*, *rogue access point*, *phishing*, dan *malware*, serta memahami langkah-langkah dasar pencegahan keamanan jaringan. Selain meningkatkan pengetahuan, kegiatan ini juga mendorong peningkatan kesadaran mahasiswa dalam menjaga keamanan data pribadi dan menerapkan kebiasaan digital yang aman. Dengan demikian, kegiatan sosialisasi ini efektif dalam meningkatkan literasi keamanan siber mahasiswa.

Kata Kunci: Keamanan Jaringan, Wi-Fi, Internet, Ancaman Siber

PENDAHULUAN

Pada kemajuan teknologi digital saat ini, penggunaan jaringan Wi-Fi dan internet sekarang menjadi bagian integral dari kehidupan modern. Hampir semua kegiatan sekarang bergantung pada koneksi jaringan, termasuk pendidikan, pekerjaan, dan hiburan. Intensitas penggunaan ini secara otomatis meningkatkan risiko terhadap berbagai ancaman keamanan siber, terutama ketika pengguna tidak memahami cara melindungi data dan perangkat mereka. Penggunaan jaringan bahwa pengguna muda dan awam seringkali terpapar risiko digital tanpa pengetahuan keamanan yang cukup, sehingga rentan terhadap penyalahgunaan informasi, *malware*, dan pencurian identitas digital. Ancaman seperti *packet sniffing*, penyadapan lalu lintas data, MITM (*man-in-the-middle*), hingga pembuatan *rogue access point* semakin sering ditemukan pada jaringan publik maupun jaringan institusi pendidikan (Zulkarnaen et al., 2025). Rendahnya kesadaran keamanan digital di kalangan pengguna, terutama pada jaringan Wi-Fi publik, menyebabkan pengguna cenderung mengabaikan praktik dasar keamanan seperti enkripsi, pemeriksaan sertifikat situs, dan pengelolaan konfigurasi jaringan yang benar (Amin et al., 2024).

Penelitian empiris menunjukkan bahwa serangan *packet sniffing* merupakan salah satu bentuk ancaman paling umum pada jaringan Wi-Fi yang tidak dikonfigurasi dengan baik, dan teknik serangan ini mampu menangkap data sensitif seperti kredensial, sesi login, maupun pola lalu lintas jaringan (Arini et al., 2023). Bahkan pada lingkungan akademik, mahasiswa yang menggunakan jaringan kampus tanpa pengamanan tambahan terbukti rentan terhadap intersepsi data dan serangan MITM jika konfigurasi enkripsi tidak sesuai standar atau perangkat tidak diperbarui secara berkala (Tamsir Ariyadi & Mubarok, 2024). Sejalan dengan itu, tinjauan sistematis mengenai keamanan Wi-Fi menegaskan bahwa evolusi protokol keamanan mulai dari WEP, WPA, WPA2, hingga WPA3 tidak terlepas dari dinamika ancaman yang terus berkembang dan celah-celah keamanan yang dimanfaatkan oleh peretas (Faíscas, 2024).

Dalam upaya untuk meningkatkan keamanan jaringan Wi-Fi kontemporer, WPA3 telah ditetapkan sebagai standar terbaru. Ini dimaksudkan untuk mengatasi kelemahan WPA2, terutama yang berkaitan dengan perlindungan terhadap serangan *brute-force.* WPA3 juga memiliki mekanisme autentikasi *Simultaneous Authentication of Equals* (SAE) yang diperkuat. Namun, studi eksperimental menunjukkan bahwa meskipun WPA3 menawarkan peningkatan signifikan, efektivitasnya tetap bergantung pada implementasi yang benar, update *firmware router*, serta pemahaman pengguna terhadap konfigurasi yang aman (Ghanim & Thanoun, 2025). Implementasi WPA3 di kampus dan lembaga pendidikan telah menunjukkan peningkatan tingkat kerentanan terhadap serangan penyusupan dan meningkatkan standar keamanan jaringan secara keseluruhan. Namun, banyak orang yang tidak memahami teknis dan tidak membuat kebijakan keamanan yang jelas.

Oleh karena itu, langkah strategis untuk meningkatkan kesiapsiagaan pengguna dalam menghadapi ancaman digital adalah mengajarkan pengguna tentang ancaman siber dan praktik pencegahan pada jaringan Wi-Fi. Sosialisasi keamanan digital yang menekankan pemahaman tentang ancaman nyata, penerapan enkripsi kontemporer, penggunaan *firewall*, dan kebiasaan digital yang aman dinilai dapat memperkuat perilaku pengguna dan mengurangi kemungkinan insiden keamanan. Oleh karena itu, penelitian ini berkonsentrasi pada pengenalan ancaman dan pencegahan serangan siber pada jaringan Wi-Fi dengan menggunakan pendekatan edukatif yang terstruktur yang memenuhi persyaratan pengguna dan sesuai dengan kemajuan protokol keamanan kontemporer.

METODE

Metode kegiatan Pengabdian Kepada Masyarakat ini dilakukan melalui sosialisasi mengenai keamanan jaringan Wi-Fi di lingkungan UIN Sulthan Thaha Saifuddin Jambi. Lokasi kegiatan sosialisasi ini adalah lantai satu Gedung Kuliah Bersama UIN Sulthan Thaha Saifuddin Jambi, Simpang Sungai Duren, Jambi Luar Kota, Muaro Jambi. Kegiatan ini ditujukan kepada mahasiswa UIN Sulthan Thaha Saifuddin Jambi dihadiri sebanyak 20 mahasiswa mahasiswa dari Program Studi Pendidikan Agama Islam (PAI).

Dalam pelaksanaan kegiatan, penyampaian materi disajikan langsung oleh Tim Pelaksana dengan menggunakan media laptop disertai sesi diskusi atau tanya jawab untuk mengetahui seberapa besar tingkat pemahaman mahasiswa dalam memahami materi yang telah disampaikan serta menambah wawasan baru yang mungkin terlewat dalam penyampaian materi. Kegiatan sosialisasi ini dilakukan dengan presentasi interaktif yang mencakup pengenalan penggunaan Wi-Fi dan Internet, Pentingnya Keamanan Jaringan, ancaman yang sangat sering terjadi dalam penggunaan jaringan Wi-Fi dan Internet, upaya-upaya menjaga keamanan jaringan Wi-Fi dan Internet serta contoh kasus beserta dampak atau kerugian dalam kehidupan modern. Tahapan pelaksanaan sosialisasi di UIN Sulthan Thaha Saifuddin Jambi adalah sebagai berikut :

Tahapan Persiapan

Penyusunan materi dimana tim pelaksana menyiapkan bahan penyuluhan yang sistematis dan relevan dengan kondisi kehidupan sehari-hari mahasiswa dalam menggunakan jaringan Wi-Fi dan juga Internet. Penyusunan materi dilakukan dengan langkah-langkah berikut:

1) Menentukan topik utama yang akan dibahas, seperti pengertian Jaringan Wi-Fi dan Internet, macam-macam serangan dalam penggunaan Wi-Fi dan Internet, ancaman yang marak atau umum terjadi, serta pencegahan atau antisipasi sederhana yang dapat diterapkan oleh mahasiswa.
2) Pengumpulan data, contoh kasus, dan informasi valid dari sumber terpercaya agar materi akurat dan tidak bersifat sekadar teori umum.
3) Penyusunan alur penyampaian materi secara bertahap, mulai dari penjelasan konsep dasar hingga pembahasan kasus nyata agar peserta mudah memahami konteksnya.

Tahapan Penyuluhan

1) Pembukaan dan Pengenalan
   Pelaksana melakukan perkenalan singkat dan dilanjutkan dengan pertanyaan pemantik sederhana agar muncul rasa ingin tahu dan kesiapan untuk mengikuti materi.
2) Penyampaian Materi
   Materi disampaikan secara interaktif melalui presentasi.
   - Pengertian Jaringan Wi-Fi dan Internet serta perannya dalam era modern.
   - Macam-macam serangan yang sering terjadi dalam jaringan, seperti *eavesdroping* (Penyadapan Sinyal), *Rouge Access Point* (Jaringan Wi-Fi Palsu), *Network Abuse* (Penyalahgunaan Jaringan) hingga *Malware*.
   - Upaya menjaga keamanan Jaringan Wi-Fi dan Internet yang dimulai dari diri sendiri.
3) Sesi Diskusi
   Tahap penyuluhan diakhiri dengan sesi diskusi sebagai bentuk evaluasi cepat terhadap materi yang telah disampaikan yang berfungsi mengukur pemahaman peserta secara langsung. Tidak hanya itu, sesi diskusi juga berfungsi untuk menambah wawasan serta menjaga suasana tetap menarik dan partisipatif.

LANDASAN TEORI

1. Keamanan Jaringan Wi-Fi dan Internet

Cisco menyatakan bahwa keamanan Wi-Fi adalah perlindungan perangkat dan jaringan yang terhubung dalam lingkungan nirkabel untuk mencegah akses oleh pihak yang tidak berwenang. Wi-Fi adalah teknologi populer yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel melalui jaringan komputer, termasuk akses internet berkecepatan tinggi, menggunakan gelombang radio (Eben et al., 2024). Kaspersky mendefinisikan keamanan internet sebagai istilah yang menggambarkan keamanan untuk aktivitas dan transaksi yang dilakukan melalui internet, termasuk keamanan peramban dan perilaku daring. Keamanan jaringan adalah konsep yang bertujuan untuk mencegah akses oleh pengguna yang tidak sah ke dalam sistem jaringan komputer (Eben et al., 2024).

Pemerintah ikut juga ikut andil dalam menjaga dan melindungi keamanan jaringan Wi-Fi dan Internet dari tangan oknum yang tidak bertanggung jawab. Dalam upaya memperkuat keamanan siber, pemerintah Indonesia telah menerbitkan berbagai regulasi dan kebijakan yang bertujuan untuk melindungi infrastruktur digital nasional. Lembaga utama yang bertanggung jawab adalah Badan Siber dan Sandi Negara (BSSN), yang bertugas menyusun kebijakan, mengamankan Infrastruktur Informasi Vital Nasional (IIVN), serta melakukan penanggulangan insiden siber.

Dari sisi kerangka hukum, upaya pemerintah diwujudkan dalam beberapa peraturan perundang-undangan penting, antara lain; Undang-Undang Nomor 1 Tahun 2024 (Perubahan Kedua atas UU ITE), UU ini mengatur hak dan kewajiban pengguna, transaksi elektronik, serta memberikan kerangka penindakan pidana terhadap aktivitas ilegal di ruang siber, seperti penyebaran konten terlarang, penipuan daring, dan pencemaran nama baik. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), memberikan kewajiban ketat bagi pihak yang mengelola data (Pengendali Data) untuk menerapkan standar keamanan dan perlindungan yang memadai, serta memberikan sanksi bagi penyalahgunaan atau kebocoran data. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber Perpres, ini menjadi pedoman strategis bagi seluruh instansi pemerintah dan pihak terkait dalam merespons, memulihkan, dan mengelola krisis yang diakibatkan oleh insiden siber.

2. Ancaman Pada Jaringan Wi-Fi dan Internet

1) Penyadapan Sinyal (*Eavesdropping*)

Tindakan mengintersep atau "menguping" data yang sedang ditransmisikan melalui jaringan. Penyadapan Sinyal (*Eavesdropping*), yang sering kali diwujudkan melalui serangan *Packet Sniffing* Mereka dapat mencuri kata sandi, email, atau percakapan. Cara kerjanya

memanfaatkan jaringan yang tidak terenkripsi untuk secara diam-diam menangkap paket data yang lewat, memungkinkan pelaku mencuri informasi sensitif seperti *username* dan *password* (Ariyadi et al., 2024).

2) **Jaringan Wi-Fi Palsu (*Rogue Access Point*)**
Rogue Access Point (RAP) merupakan sebuah AP yang dipasang pada sebuah jaringan terkendali tanpa sebuah otorisasi dari *network management*. RAP juga dapat dipasang pada sebuah jaringan yang telah dimanipulasi agar penyerang dapat masuk ke dalam jaringan tertentu (Utama et al., 2020). Pelaku RAP biasanya juga membuat jaringan Wi-Fi palsu dengan nama yang mirip jaringan resmi sehingga ketika kita terhubung, semua data kita bisa dicuri.
3) **Penyalahgunaan Jaringan (*Network Abuse*)**
Penggunaan jaringan untuk tujuan ilegal atau tidak etis. Contoh penyalahgunaan jaringan melakukan pencurian data, distribusi *malware* hingga Serangan DDoS (*Distributed Denial of Service*) pelaku dapat mengambil alih perangkat yang terhubung ke jaringan (menjadikannya bot) untuk melakukan serangan ke server atau situs web lain.
4) **Serangan MITM (*Man-in-the-Middle*)**
Serangan MITM adalah jenis serangan yang memanfaatkan celah dalam jaringan untuk memantau, mengubah, atau mencuri data yang dikirimkan antara dua entitas yang berkomunikasi (Firmansyah, 2023). Pelaku menyusup di antara perangkat Anda dan situs web yang kalian kunjungi. Penyerang MITM menyusup dalam aliran komunikasi dan meniru salah satu pihak, sehingga mereka dapat memperoleh akses tidak sah ke informasi sensitif.
5) ***Phising***
Phishing merupakan tindakan penipuan yang dilakukan secara daring dengan tujuan memperoleh informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dari korban dengan mencuri identitas, merampas dana, atau merusak reputasi (Lokapala et al., 2024). Pelaku phishing dapat menggunakan cara melalui email phishing untuk mendapatkan data pribadi denganmenyamar sebagai orang atau organisasi yang berwenang melalui email. Mengutip data yang bersumber dari Badan Siber dan Sandi Negara (BSSN) terdapat 164.131 kasus email phishingyang terjadi di Indonesia pada tahun 2022.
6) **Malware (*Malicious Software*)**
Malware merupakan kependekan dari malicious software, yaitu perangkat lunak berbahaya yang dirancang untuk menyusup ke dalam sistem tanpa diketahui oleh pemiliknya dan dapat bertahan dalam jangka waktu tertentu. *Malware* biasanya masuk melalui email, file unduhan, atau program yang sudah terinfeksi. Sebagian besar kejahatan komputer terjadi dalam bentuk pencurian data pribadi atau pembuatan *backdoor* yang memungkinkan pelaku mengakses komputer tanpa izin. Setiap perangkat lunak yang menjalankan tindakan tersebut tanpa persetujuan pemilik perangkat dapat dikategorikan sebagai *malware*(Sari, 2024).

3. Tips Menjaga Keamanan Jaringan Wi-Fi dan Internet

1) Gunakan VPN (*Virtual Private Network*), Selalu nyalakan VPN saat terhubung ke Wi-Fi publik. VPN akan mengenkripsi data kita sehingga tidak bisa dibaca oleh peretas.
2) Periksa HTTPS: Pastikan situs web yang di kunjungi menggunakan https://, bukan http://.
3) Waspadai jaringan Wi-Fi palsu selalu verifikasi nama Wi-Fi publik dengan staf tempat tersebut. Nonaktifkan fitur sambung otomatis ke jaringan Wi-Fi di perangkat.
4) Amankan router pribadi dengan mengubah kata sandi bawaan router serta sembunyikan jaringan wifi (SSID) dan gunakan enkripsi WPA2 atau WPA3 yang kuat.
5) Perbarui perangkat lunak secara rutin dengan selalu memperbarui sistem operasi, aplikasi, dan *firmware router* untuk menutup celah keamanan
6) Pasang *antivirus*, gunakan perangkat lunak *antivirus* dan *anti-malware* yang terpercaya dan selalu perbarui definisinya.

7) Berhati-hati dengan email dan tautan jangan pernah mengklik tautan atau mengunduh lampiran dari sumber yang tidak dikenal atau mencurigakan.
8) Gunakan kata sandi kuat, dengan menggunakan kata sandi unik dan rumit untuk setiap akun.
9) Atur jam pengunaan internet dan maksimal perangkat yang bisa mengaksesnya.

HASIL DAN PEMBAHASAN

Berdasarkan hasil pengamatan kegiatan sosialisasi, peserta menunjukkan antusiasme yang tinggi terutama pada sesi pemaparan materi terkait ancaman siber yang sering terjadi pada jaringan Wi-Fi publik, seperti penyadapan sinyal (*eavesdropping*), Wi-Fi palsu (*rogue access point*), *phishing*, dan *malware*. Sebagian besar peserta mengakui bahwa sebelumnya mereka belum memahami secara mendalam mengenai risiko keamanan yang dapat muncul saat menggunakan jaringan Wi-Fi publik tanpa perlindungan tambahan. Kegiatan penyampaian materi dilakukan secara langsung dan interaktif sebagaimana ditunjukkan pada Gambar 1.

Gambar 1. Penyampaian materi sosialisasi keamanan jaringan Wi-Fi dan internet kepada mahasiswa Program Studi Pendidikan Agama Islam (PAI).

Pada sesi diskusi dan tanya jawab, terlihat adanya peningkatan pemahaman peserta terhadap materi yang disampaikan. Hal ini *ditunjukkan* melalui kemampuan peserta dalam menjelaskan kembali jenis-jenis ancaman siber serta menyebutkan langkah-langkah dasar pencegahan, seperti penggunaan VPN, kewaspadaan terhadap jaringan Wi-Fi yang tidak dikenal, pemeriksaan keamanan situs web melalui protokol HTTPS, serta pentingnya pembaruan perangkat lunak secara berkala. Dari hasil diskusi, sebagian besar peserta menyatakan baru mengetahui bahwa jaringan Wi-Fi palsu dapat menyerupai jaringan resmi dan berpotensi digunakan untuk mencuri data pribadi. Antusiasme dan partisipasi aktif peserta selama diskusi dapat dilihat pada Gambar 2.

Gambar 2. Foto bersama tim pelaksana dan peserta kegiatan sosialisasi keamanan jaringan Wi-Fi dan internet.

Selain itu, kegiatan sosialisasi ini juga memberikan dampak positif terhadap perubahan sikap dan kesadaran digital peserta. Mahasiswa mulai memahami pentingnya menjaga kerahasiaan data pribadi dan menerapkan kebiasaan digital yang aman, khususnya saat mengakses internet melalui jaringan publik. Pendekatan edukatif yang disampaikan secara interaktif dinilai efektif dalam menyampaikan materi keamanan jaringan yang bersifat teknis agar mudah dipahami oleh peserta dari latar belakang non-teknologi informasi.

Secara keseluruhan, hasil kegiatan menunjukkan bahwa sosialisasi keamanan jaringan Wi-Fi dan internet mampu menjadi sarana edukasi yang efektif dalam meningkatkan literasi keamanan siber mahasiswa. Kegiatan ini tidak hanya menambah pengetahuan peserta, tetapi juga mendorong terbentuknya perilaku yang lebih waspada dan bertanggung jawab dalam memanfaatkan teknologi jaringan di lingkungan akademik.

KESIMPULAN

Pengenalan ancaman dan pencegahan serangan siber melalui edukasi keamanan jaringan Wi-Fi dan internet merupakan langkah strategis dalam meningkatkan kesiapsiagaan pengguna terhadap risiko keamanan digital. Kegiatan ini menegaskan pentingnya pemahaman dasar mengenai ancaman siber dan penerapan praktik keamanan jaringan dalam mendukung penggunaan teknologi secara aman dan bertanggung jawab. Melalui kegiatan edukatif yang terstruktur, diharapkan literasi keamanan siber di lingkungan akademik dapat terus meningkat dan mendorong terbentuknya budaya penggunaan internet yang lebih aman di kalangan mahasiswa.

DAFTAR PUSTAKA

Amin, M. Y., Isnaeni, D., & Sri Utami, N. (2024). Legal protection of public WiFi users from cyber crime. Jurnal Mercatoria, 17(2), 217–226.pdf.

Arini, Arsalan, M., & Teja Sukmana, H. (2023). Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co) (Vol. 6, Issue 2).

Ariyadi, T., Irwansyah, & Huda, M. S. (2024). Analisis Keamanan Jaringan Wifi Mahasiswa UBD Dari Serangan Packet Sniffing. 3.

Eben, Mukramin, & Abduh, H. (2024). Pengembangan Manajemen Keamanan Jaringan Nirkabel (WIFI) Menggunakan Routerboard Mikrotik dan Firewall pada SMK Kristen Palopo. 12(3).

Faíscas, D. (2024). Advanced Research on Information Systems Security (In)Security in Wi-Fi networks: a systematic review.

Firmansyah, D. (2023). PENERAPAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI SERANGAN MAN IN THE MIDDLE. 1(1), 73–80.

Ghanim, A. A., & Thanoun, M. Y. (2025). Evaluating the effectiveness of WPA3 protocol against advanced hacking attacks. International Journal of Wireless and Microwave Technologies (IJWMT).

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. 5(1), 19–24.

Sari, R. P. (2024). Apa itu Malware? Jenis dan Cara Pencegahannya. Cloud Computing Indonesia. https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-malware-jenis

Tamsir Ariyadi, I. I., & Mubarok, M. S. H. (2024). Analisis keamanan jaringan Wi-Fi mahasiswa UBD dari serangan packet sniffing. Jurnal Ilmiah Informatika.

Utama, D. S., Kartikasari, D. P., & Bakhtiar, F. A. (2020). Implementasi Metode Multi-Agent Untuk Mendeteksi Rogue Access Point (RAP). 4(9), 3108–3120.

Zulkarnaen, I., R, M. Z. M., Syarifudin, S., Rinaldi, S., & Akem, U. (2025). Wireless Fidelity Network Security Threats (Wi-Fi). JERIT: Journal of Educational Research and Innovation Technology, 2(2), 73–82. https://doi.org/10.34125/jerit.v2i2.26