

Analisis Tingkat Kesadaran Pengguna Terhadap Keamanan Jaringan Wi-Fi di Lingkungan Kampus

Zahara Putri Nurliati¹, Reva Unieq Faizila², Salsabila Adine Susyantika³, Nicolas Ricardo⁴, Imaduddin Ali Muhammad⁵, Fiqhi Trysandi Naufal⁶, Rayhan Aditya⁷

^{1,2,3,4,5,6,7}Program Studi Teknik Komputer, Institut Teknologi Batam, Indonesia

Informasi Artikel

Terbit: Juli 2026

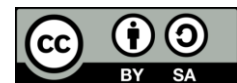
Kata Kunci:

Keamanan Informasi
Keamanan Wi-Fi
Kesadaran Pengguna
Mahasiswa
Perilaku Keamanan

ABSTRAK

Penelitian ini bertujuan untuk menganalisis tingkat kesadaran pengguna terhadap keamanan jaringan Wi-Fi di lingkungan kampus, mengingat tingginya risiko serangan siber seperti sniffing dan phishing pada jaringan publik. Penelitian ini menggunakan metode kuantitatif deskriptif dengan pengumpulan data melalui kuesioner kepada 54 mahasiswa yang dipilih menggunakan teknik *accidental sampling*. Analisis data dilakukan menggunakan statistik deskriptif untuk mengukur rata-rata skor pada empat aspek kesadaran. Hasil penelitian menunjukkan adanya kesenjangan signifikan antara pemahaman konsep dan praktik di lapangan. Aspek Pengetahuan dan Sikap responden berada pada kategori tinggi dengan nilai rata-rata masing-masing 3,80 dan 4,04, yang mengindikasikan bahwa mahasiswa memahami risiko keamanan data. Namun, aspek Perilaku serta Kebiasaan dan Pengalaman berada pada kategori yang lebih rendah dengan rata-rata 3,13 dan 3,00. Hal ini menunjukkan bahwa pemahaman teori belum sepenuhnya diterapkan dalam tindakan pencegahan nyata, seperti penggunaan VPN atau penggantian kata sandi secara rutin. Penelitian ini merekomendasikan perlunya peningkatan edukasi yang bersifat praktis untuk mengubah kesadaran kognitif menjadi perilaku keamanan yang konsisten.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Zahara Putri Nurliati,
Email: zaharaputrinurliati@gmail.com

1. PENDAHULUAN

Konektivitas internet melalui jaringan nirkabel (Wi-Fi) telah menjadi infrastruktur krusial dalam mendukung aktivitas pembelajaran, penelitian, serta komunikasi akademik di perguruan tinggi. Mahasiswa dan dosen sangat bergantung pada jaringan Wi-Fi untuk mengakses sumber belajar digital, sistem informasi akademik, dan platform kolaborasi daring yang membutuhkan koneksi cepat dan stabil [1]. Selain itu, ketersediaan jaringan yang luas dan andal juga menjadi indikator kesiapan infrastruktur digital perguruan tinggi dalam menghadapi transformasi teknologi dan pembelajaran berbasis digital [2].

Meskipun memiliki peran penting, jaringan Wi-Fi di lingkungan kampus menghadapi berbagai ancaman keamanan yang serius. Ancaman seperti packet sniffing, man-in-the-middle attack, Evil Twin, serta rekayasa sosial (phishing) berpotensi mengganggu kerahasiaan dan integritas data pengguna. Penelitian menunjukkan bahwa serangan Evil Twin mampu mengecoh pengguna agar terhubung ke access point palsu sehingga memungkinkan pencurian informasi sensitif tanpa disadari oleh korban [3]. Kondisi ini menunjukkan bahwa jaringan nirkabel kampus sangat rentan dieksploitasi apabila tidak dikelola dan diamankan secara optimal.

Risiko keamanan jaringan Wi-Fi semakin meningkat akibat rendahnya kesadaran pengguna terhadap praktik keamanan informasi. Sebagian besar mahasiswa belum memahami langkah dasar dalam menjaga keamanan data, seperti penggunaan kata sandi yang kuat, pembaruan perangkat lunak, serta kehati-hatian saat menggunakan jaringan publik [4], [5]. Penelitian lain juga mengungkapkan bahwa banyak pengguna mengalami kesulitan dalam mengenali tanda-tanda serangan phishing atau jaringan Wi-Fi palsu, sehingga meningkatkan potensi kebocoran data pribadi [6]. Rendahnya tingkat kesadaran ini menjadikan faktor manusia sebagai salah satu kelemahan utama dalam sistem keamanan siber di lingkungan kampus.

Berbagai pendekatan teknis telah dikembangkan untuk meningkatkan keamanan jaringan Wi-Fi, antara lain penerapan firewall, pembaruan sistem secara berkala, serta penggunaan protokol keamanan yang lebih mutakhir seperti WPA3 [7]. Namun, efektivitas teknologi tersebut sangat bergantung pada perilaku dan kesadaran pengguna jaringan. Beberapa studi menunjukkan bahwa mahasiswa masih sering menggunakan kata sandi yang lemah, terhubung ke jaringan terbuka tanpa verifikasi, serta mengabaikan keamanan saat mengakses layanan penting melalui Wi-Fi kampus [8]. Edukasi dan sosialisasi terbukti mampu meningkatkan pemahaman pengguna mengenai identitas digital dan praktik keamanan dasar dalam penggunaan jaringan nirkabel [9].

Perilaku pengguna memiliki pengaruh signifikan terhadap tingkat keamanan jaringan Wi-Fi. Banyak insiden keamanan terjadi akibat kelalaian pengguna, seperti mengklik tautan mencurigakan, terhubung ke jaringan tanpa enkripsi, atau melakukan autentikasi pada jaringan umum. Penelitian terkait perilaku mahasiswa terhadap ancaman phishing menunjukkan bahwa pengguna yang memiliki persepsi risiko tinggi cenderung lebih berhati-hati dalam menggunakan internet [10]. Selain itu, perilaku keamanan juga dipengaruhi oleh faktor individu dan lingkungan, seperti tingkat literasi digital, pengalaman pengguna, kebijakan kampus, serta budaya keamanan yang diterapkan [11].

Berdasarkan permasalahan tersebut, penelitian ini menjadi inovatif karena tidak hanya meninjau aspek teknis keamanan jaringan Wi-Fi, tetapi juga menganalisis tingkat kesadaran, pengetahuan, dan perilaku pengguna dalam menghadapi risiko keamanan. Hasil penelitian ini diharapkan dapat menjadi dasar dalam penyusunan kebijakan keamanan informasi serta pengembangan program edukasi literasi digital yang lebih efektif di lingkungan perguruan tinggi.

2. METODE PENELITIAN

2.1. Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif untuk memperoleh gambaran faktual mengenai tingkat kesadaran mahasiswa terhadap keamanan jaringan Wi-Fi di lingkungan kampus. Pendekatan ini dipilih karena mampu menghasilkan data yang terstruktur dan memungkinkan analisis numerik terkait pengetahuan, sikap, serta perilaku pengguna. Metode penelitian ini mengacu pada kerangka metodologis pengukuran kesadaran keamanan siber pada mahasiswa yang dijelaskan dalam literatur terkait [12].

2.2. Populasi dan Sampel

Populasi penelitian mencakup seluruh mahasiswa yang memanfaatkan jaringan Wi-Fi kampus. Penentuan sampel dilakukan dengan teknik *accidental sampling*, yaitu pengambilan responden berdasarkan siapa saja yang menerima dan bersedia mengisi kuesioner tanpa kriteria khusus. Teknik ini digunakan karena distribusi kuesioner dilakukan secara online kepada mahasiswa dari berbagai program studi. Sebanyak 54 responden berhasil berpartisipasi, dengan data identitas yang meliputi nama, jenis kelamin, usia, program studi serta frekuensi penggunaan jaringan Wi-Fi.

2.3. Instrumen Penelitian

Instrumen penelitian menggunakan kuesioner skala Likert lima poin dengan kategori: 1 = Sangat Tidak Setuju, 2 = Tidak Setuju, 3 = Netral, 4 = Setuju, 5 = Sangat Setuju. Mencakup empat aspek utama, yaitu:

1. Pengetahuan tentang Keamanan Wi-Fi
Mengukur pemahaman responden mengenai risiko dan konsep dasar keamanan jaringan Wi-Fi.
2. Sikap terhadap Keamanan Wi-Fi
Menilai kepedulian dan pandangan responden tentang pentingnya menjaga keamanan saat menggunakan Wi-Fi.
3. Perilaku pengguna Wi-Fi
Menggambarkan tindakan nyata responden dalam menerapkan langkah-langkah keamanan ketika mengakses jaringan.
4. Kebiasaan dan Pengalaman Penggunaan Wi-Fi
Menilai pola penggunaan Wi-Fi serta pengalaman responden terkait insiden atau potensi risiko keamanan.

2.4. Teknik Pengumpulan Data

Pengumpulan data dilakukan secara daring melalui penyebaran tautan Google Form kepada mahasiswa melalui grup kelas dan platform komunikasi internal kampus. Responden diberikan waktu pengisian selama periode tertentu hingga jumlah minimal terpenuhi. Responden hanya diperbolehkan mengisi satu kali untuk menjaga keaslian data.

2.5. Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan analisis deskriptif kuantitatif. Langkah pertama yaitu melakukan uji validitas dan reliabilitas untuk memastikan bahwa setiap butir pernyataan layak digunakan. Analisis dilanjutkan dengan menghitung frekuensi dan persentase jawaban dari setiap item, serta nilai rata-rata (mean) untuk mengukur tingkat kesadaran pengguna terhadap keamanan jaringan Wi-Fi. Kategori tingkat kesadaran ditentukan berdasarkan nilai rata-rata skor, yaitu:

1,00–2,33 = Rendah, 2,34–3,66 = Sedang, dan 3,67–5,00 = Tinggi.

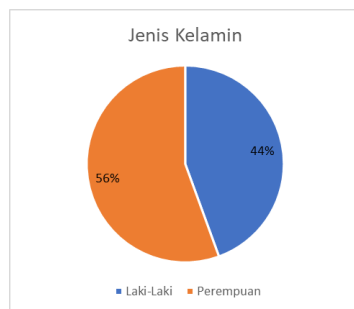
Hasil analisis disajikan dalam bentuk tabel dan grafik agar memudahkan interpretasi data.

2.6. Lokasi Penelitian dan Waktu Penelitian

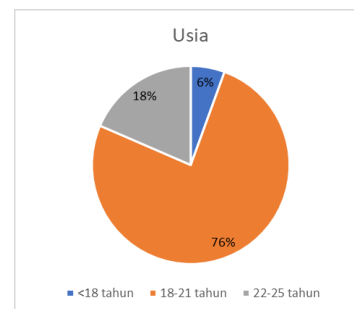
Penelitian dilaksanakan di lingkungan kampus pada periode September 2025, dengan seluruh proses penyebaran instrumen dan pengumpulan data dilakukan secara daring melalui Google Form.

3. HASIL DAN ANALISIS

Bagian ini diawali dengan pemaparan data demografis responden sebagai dasar interpretasi hasil penelitian. Distribusi responden berdasarkan jenis kelamin, usia, dan frekuensi penggunaan Wi-Fi disajikan pada diagram berikut.

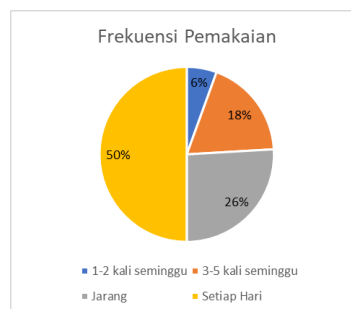


Gambar 1 Distribusi partisipan berdasarkan Kelamin



Gambar 2 Distribusi partisipan berdasarkan Usia

Penelitian ini bertujuan untuk menganalisis tingkat kesadaran pengguna terhadap keamanan jaringan Wi-Fi di lingkungan kampus. Sebanyak 54 responden berpartisipasi dalam survei ini, terdiri dari 24 laki-laki (44,4%) dan 30 perempuan (55,6%). Mayoritas responden berusia 18–21 tahun (75,9%), sedangkan 18,5% berusia 22–25 tahun, dan 5,6% di bawah 18 tahun. Berdasarkan frekuensi penggunaan, 50% responden menggunakan Wi-Fi kampus setiap hari, diikuti oleh 25,9% yang jarang, 18,5% menggunakan 3–5 kali per minggu, dan 5,6% hanya 1–2 kali per minggu. Temuan ini menunjukkan bahwa sebagian besar mahasiswa merupakan pengguna aktif jaringan Wi-Fi kampus, sehingga kesadaran terhadap aspek keamanannya menjadi topik yang relevan untuk diteliti.



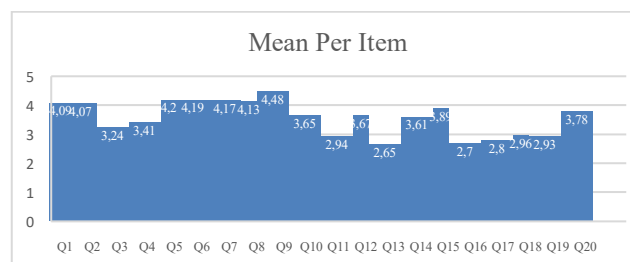
Gambar 3 Gambar Frekuensi Pemakaian Wi-Fi Kampus

3.1. Analisis Deskriptif Kesadaran Keamanan Wi-Fi

Tabel 1 Statistik Deskriptif Item Kesadaran Keamanan Wi-Fi

Item	Min	Max	Mean	Std. Deviation	Skewness
Q1	2	5	4,09	0,875	-0,36
Q2	2	5	4,07	0,866	-0,509
Q3	1	5	3,24	1,212	-0,022
Q4	1	5	3,41	1,158	-0,41
Q5	1	5	4,2	1,053	-1,332
Q6	3	5	4,19	0,848	-0,37
Q7	2	5	4,17	0,885	-0,679
Q8	2	5	4,13	0,933	-0,557
Q9	3	5	4,48	0,818	-1,119
Q10	1	5	3,65	1,102	-0,568
Q11	1	5	2,94	1,28	0,107
Q12	1	5	3,67	1,166	-0,495
Q13	1	5	2,65	1,32	0,28
Q14	1	5	3,61	1,204	-0,406
Q15	1	5	3,89	1,208	-0,713
Q16	1	5	2,7	1,423	0,305
Q17	1	5	2,8	1,172	0,048
Q18	1	5	2,96	1,288	-0,094
Q19	1	5	2,93	1,399	0,094
Q20	1	5	3,78	1,093	-0,528

Berdasarkan hasil analisis deskriptif, nilai rata-rata setiap item berada pada rentang 2,65 hingga 4,48, menunjukkan adanya variasi tingkat kesadaran antarresponden. Jika menggunakan kategori klasifikasi mean (1,00–2,33 = rendah; 2,34–3,66 = sedang; dan 3,67–5,00 = tinggi), maka sebagian besar pernyataan berada pada kategori tinggi, terutama yang berkaitan dengan persepsi terhadap pentingnya keamanan Wi-Fi. Item dengan nilai tertinggi adalah Q9 (“Saya yakin pihak kampus perlu meningkatkan keamanan jaringan Wi-Fi”) dengan mean 4,48, menandakan kuatnya perhatian mahasiswa terhadap aspek keamanan jaringan di kampus. Item Q5 (mean = 4,20) dan Q6 (mean = 4,19) juga berada pada kategori tinggi, yang memperlihatkan bahwa sebagian besar mahasiswa telah cukup terpapar isu-isu keamanan Wi-Fi dan memahami urgensinya dalam aktivitas sehari-hari.



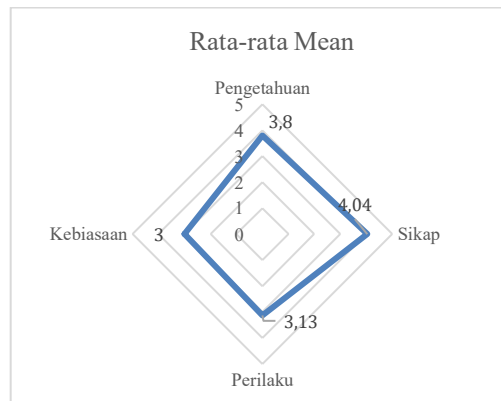
Gambar 4 Rata-Rata Skor Setiap Item Kesadaran Wi-Fi

Beberapa item yang berkaitan dengan pemahaman teknis berada pada kategori sedang, misalnya Q3 (memeriksa keamanan jaringan yang digunakan, mean = 3,24) dan Q4 (pemahaman terhadap protokol WPA2/WPA3, mean = 3,41). Hal ini menunjukkan bahwa meskipun mahasiswa menyadari pentingnya menjaga keamanan jaringan, kemampuan mereka dalam hal teknis tidak sekuat kesadarannya secara umum. Keterbatasan ini wajar mengingat tidak semua mahasiswa memiliki latar belakang teknologi informasi atau pengalaman teknis yang memadai.

Nilai mean terendah terlihat pada Q13 (penggunaan VPN, mean = 2,65) dan Q16 (pengalaman gangguan atau serangan, mean = 2,70), keduanya berada pada kategori sedang namun mendekati rendah. Rendahnya penggunaan VPN mencerminkan bahwa praktik pengamanan tambahan masih belum menjadi kebiasaan umum di kalangan mahasiswa. Selain itu, minimnya pengalaman insiden keamanan dapat membuat sebagian mahasiswa merasa bahwa risiko serangan tidak terlalu dekat dengan kehidupan mereka. Temuan ini

memperlihatkan adanya perbedaan antara kesadaran konseptual dan penerapan perilaku keamanan, sehingga edukasi mengenai praktik keamanan digital tetap diperlukan.

3.2. Pengetahuan, Sikap, Perilaku, serta Kebiasaan dan Pengalaman Pengguna



Gambar 5 Nilai Rata-Rata Empat Aspek (Pengetahuan, Sikap, Perilaku, Kebiasaan & Pengalaman)

Berdasarkan pengelompokan pertanyaan, aspek pengetahuan (Q1–Q5) memperlihatkan tingkat kesadaran yang tinggi. Responden memahami bahwa jaringan Wi-Fi dapat menjadi target serangan (Q1, mean = 4,09) dan menyadari risiko penggunaan Wi-Fi publik yang tidak terenkripsi (Q2, mean = 4,07). Mereka juga banyak yang telah terpapar informasi terkait kasus pencurian data melalui Wi-Fi (Q5, mean = 4,20). Meskipun demikian, pemahaman teknis seperti cara mengecek keamanan jaringan (Q3, mean = 3,24) dan arti protokol keamanan WPA2/WPA3 (Q4, mean = 3,41) masih berada pada kategori sedang, menandakan bahwa tidak semua mahasiswa memiliki pengetahuan teknis yang memadai.

Pada aspek sikap (Q6–Q10), kecenderungan positif terlihat cukup konsisten. Mahasiswa menilai pentingnya memperhatikan keamanan saat menggunakan Wi-Fi kampus (Q6, mean = 4,19), serta percaya bahwa keamanan jaringan berpengaruh terhadap privasi data pengguna (Q7, mean = 4,17). Selain itu, mereka menyatakan kehati-hatian saat mengakses situs penting dengan jaringan publik (Q8, mean = 4,13) dan menilai perlunya peningkatan keamanan oleh pihak kampus (Q9, mean = 4,48). Namun, persepsi terhadap keamanan Wi-Fi kampus sendiri masih bervariasi (Q10, mean = 3,65).

Untuk aspek perilaku (Q11–Q15), hasilnya cenderung lebih rendah dibanding dua aspek sebelumnya. Kebiasaan mengganti kata sandi setelah menggunakan Wi-Fi umum (Q11, mean = 2,94) dan penggunaan VPN (Q13, mean = 2,65) masih jarang dilakukan. Di sisi lain, beberapa tindakan seperti menghindari akses data pribadi pada jaringan kampus (Q12, mean = 3,67) dan tidak membagikan kata sandi Wi-Fi kepada orang lain (Q15, mean = 3,89) menunjukkan perilaku kehati-hatian yang lebih baik. Secara keseluruhan, aspek perilaku menunjukkan bahwa pengetahuan dan sikap positif belum sepenuhnya diterjemahkan ke dalam tindakan rutin.

Aspek terakhir, yaitu kebiasaan dan pengalaman pengguna (Q16–Q20), memperlihatkan nilai yang lebih moderat. Pengalaman langsung terkait gangguan keamanan (Q16, mean = 2,70) maupun kecenderungan mengabaikan peringatan keamanan (Q17, mean = 2,80) menunjukkan bahwa sebagian responden belum sepenuhnya menyadari pentingnya praktik keamanan digital. Kebiasaan logout setelah menggunakan jaringan umum (Q18, mean = 2,96) dan partisipasi dalam pelatihan keamanan jaringan (Q19, mean = 2,93) juga masih rendah. Meski demikian, adanya rasa tanggung jawab untuk menjaga keamanan data (Q20, mean = 3,78) menandakan bahwa sebagian mahasiswa memiliki kesadaran etis meskipun belum didukung oleh kebiasaan yang kuat.

3.3. Praktik Keamanan dan Pengalaman Risiko

Hasil analisis menunjukkan bahwa sebagian kecil responden pernah mengalami gangguan keamanan saat menggunakan Wi-Fi kampus (Q16, mean = 2,70) maupun mengikuti pelatihan keamanan jaringan (Q19, mean = 2,93). Minimnya pengalaman langsung dan paparan pelatihan dapat menjadi salah satu faktor mengapa sebagian perilaku pencegahan belum dilakukan secara rutin. Pada aspek praktik keamanan, item seperti penggunaan antivirus aktif (Q14, mean = 3,61) dan kebiasaan logout setelah memakai Wi-Fi umum atau kampus (Q18, mean = 2,96) menunjukkan bahwa sebagian mahasiswa mulai menerapkan langkah-langkah perlindungan, meskipun belum sepenuhnya konsisten. Secara umum, temuan ini memperlihatkan bahwa kesadaran tidak selalu berbanding lurus dengan tindakan, terutama ketika mahasiswa belum pernah mengalami langsung konsekuensi dari ancaman keamanan digital.

3.4. Interpretasi Umum

Tabel 2 Rata-Rata Setiap Aspek Kesadaran Keamanan Wi-Fi

Aspek	Rata-rata Mean
Pengetahuan	3,80
Sikap	4,04
Perilaku	3,13
Kebiasaan & Pengalaman	3,00

Secara umum, aspek pengetahuan dan sikap berada pada kategori tinggi hingga cukup tinggi, mencerminkan bahwa mahasiswa telah memahami risiko penggunaan Wi-Fi serta pentingnya menjaga keamanan data. Namun, aspek perilaku dan kebiasaan memiliki nilai yang lebih rendah, mengindikasikan bahwa tindakan nyata yang dilakukan mahasiswa belum sejalan dengan tingkat pengetahuan dan sikap mereka.

Distribusi nilai skewness yang sebagian besar negatif menunjukkan kecenderungan responden memberi skor lebih tinggi pada pernyataan positif, terutama pada aspek pengetahuan dan sikap. Akan tetapi, nilai mean yang relatif rendah pada indikator kebiasaan teknis seperti penggunaan VPN, pelatihan keamanan, atau pengalaman menghadapi serangan, menunjukkan perlunya peningkatan pemahaman praktis dan pembiasaan perilaku keamanan digital. Secara keseluruhan, hasil ini menunjukkan bahwa kesadaran mahasiswa terhadap keamanan jaringan lebih kuat pada aspek kognitif dan afektif, sementara aspek tindakan dan pengalaman masih memerlukan pendampingan, pelatihan, serta kebijakan kampus yang dapat mendorong perilaku keamanan yang lebih konsisten.

4. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa tingkat kesadaran pengguna terhadap keamanan jaringan Wi-Fi di lingkungan kampus menunjukkan variasi yang signifikan antar aspek. Secara kognitif dan afektif, mahasiswa memiliki kesadaran yang tinggi; hal ini dibuktikan dengan skor rata-rata aspek Pengetahuan (3,80) dan Sikap (4,04) yang tinggi. Responden terbukti memahami risiko penggunaan Wi-Fi publik serta menyadari pentingnya menjaga privasi data mereka.

Akan tetapi, tingginya pengetahuan tersebut belum berbanding lurus dengan tindakan nyata di lapangan. Aspek Perilaku dan Kebiasaan memiliki skor yang lebih rendah, yaitu 3,13 dan 3,00. Temuan ini menegaskan bahwa meskipun mahasiswa mengetahui bahaya yang ada, mereka cenderung belum menerapkan langkah pencegahan teknis secara konsisten, seperti penggunaan VPN atau penggantian kata sandi berkala. Faktor minimnya pengalaman langsung terkena serangan siber juga berkontribusi pada rendahnya kewaspadaan praktis ini.

Oleh karena itu, penelitian ini menyarankan agar pihak kampus tidak hanya berfokus pada penyediaan infrastruktur yang aman, tetapi juga aktif menyelenggarakan pelatihan atau sosialisasi yang bersifat teknis dan praktis guna mengubah pengetahuan menjadi kebiasaan aman. Penelitian selanjutnya diharapkan dapat memperluas jangkauan responden atau menggunakan metode kualitatif untuk menggali lebih dalam alasan psikologis di balik kesenjangan antara pengetahuan dan perilaku keamanan mahasiswa.

DAFTAR PUSTAKA

- [1] M. Singson and Rajesh, "Awareness and use of Wi-Fi infrastructure in student ' s community : a case study Pondicherry University on campus students".
- [2] A. N. Iman and M. Sholeh, "Analisis Keamanan Jaringan Wifi di MI Inwanul Huda," vol. 9, no. 2502, pp. 67–73, 2024.
- [3] I. Palamà, A. Amici, G. Bellicini, F. Gringoli, F. Pedretti, and G. Bianchi, "Attacks and vulnerabilities of Wi-Fi Enterprise networks : User security awareness assessment through credential stealing attack experiments," *Comput. Commun.*, vol. 212, no. September, pp. 129–140, 2023, doi: 10.1016/j.comcom.2023.09.031.
- [4] I. Dunder, S. Seljan, and M. Odak, "Information Security Awareness in the University Environment : A Focus on Undergraduates," vol. 14, no. 2, pp. 1621–1628, 2025, doi: 10.18421/TEM142.
- [5] M. H. N and R. Bisma, "Persepsi Keamanan Data Dan Privasi Pada Pengguna Layanan Wifi Gratis Di Coffee Shop," *JEISBI (Journal Emerg. Inf. Syst. Bus. Intell.)*, vol. 04, no. 02, pp. 164–172, 2023.
- [6] W. Aljohani and N. Elfadil, "Measuring Cyber Security Awareness of Students : A Case Study at Fahad Bin Sultan University," *Int. J. Comput. Sci. Mob. Comput.*, vol. 9, no. 6, pp. 141–155, 2020.

Analisis Tingkat Kesadaran Pengguna Terhadap Keamanan Jaringan Wi-Fi di Lingkungan Kampus (Zahara Putri Nurliati)

- [7] Eben, Mukramin, and H. Abduh, "PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO," *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 12, no. 3, 2024.
- [8] T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," vol. 14, no. September, pp. 163–173, 2024, doi: 10.34010/jati.v14i2.
- [9] I. Dan, P. Kata, S. Aman, P. Mahasiswa, and U. I. N. Sts, "Peningkatan kesadaran keamanan digital melalui sosialisasi manajemen identitas dan penggunaan kata sandi aman pada mahasiswa uin sts jambi," vol. 11, no. 8, 2025.
- [10] A. K. Gwenthure, "University students ' security behavior against email phishing attacks : insights from the health belief model," *J. Cybersecurity*, vol. 11, 2025, doi: 10.1093/cybsec/tyaf034.
- [11] I. Security, "Individual and Contextual Variables of Cyber Security Behaviour," no. 190230551, 2022.
- [12] R. Raju, N. Hidayah, A. Rahman, and A. Ahmad, "Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution," 2022.