Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

ANALISIS KETIDAKSEDARAN PELAJAR TERHADAP RISIKO KESELAMATAN DALAM PENGGUNAAN RANGKAIAN WI-FI AWAM

ANALYSIS OF STUDENT UNAWARENESS OF SECURITY RISKS IN THE USE OF PUBLIC WI-FI NETWORKS

Norazlina Abdullah[1]
Qutubuddin Buzurgoon Hassan[2]

[1] Politeknik Besut Terengganu (E-mail: azlina@polibesut.edu.my)
[2] Politeknik Besut Terengganu (E-mail: buzurgoon@polibesut.edu.my)

Article history
Received date : 2-3-2026
Revised date : 3-3-2026
Accepted date : 1-4-2026
Published date : 10-4-2026

To cite this document:
Abdullah, N., & Hassan, Q. B. (2026). Analisis ketidaksedaran pelajar terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam. *Jurnal Penyelidikan Sains Sosial (JOSSR),* 9 (29), 41 – 48.

Abstrak: *Objektif kajian ini dijalankan adalah untuk menilai sejauh mana tahap ketidaksedaran seseorang terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dan mengenal pasti pengalaman terkena penipuan (scam) dalam kalangan pelajar di samping itu, kajian ini dijalankan untuk mengenal pasti sama ada terdapat hubungan antara ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam terhadap pengalaman terkena penipuan (scam) dalam talian dalam kalangan pelajar. Sampel kajian yang dipilih adalah dalam kalangan pelajar institusi pengajian tinggi. Sampel pelajar dipilih kerana umumnya sebahagian pelajar selalu mempunyai masalah kewangan dan kekangan dari segi kemampuan untuk membeli kuota data internet. Kajian ini menggunakan pendekatan berbentuk kuantitatif yang dijalankan melalui kaedah tinjauan. Sampel terdiri daripada pelajar di Politeknik Besut Terengganu. Teknik pensampelan yang digunakan adalah melalui teknik pensampelan rawak. Data yang di kumpul akan dianalisis menggunakan analisis deskriptif untuk menentukan tahap ketidaksedaran pelajar terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam. Manakala analisis menggunakan regresi linear untuk menentukan hubungan antara pemboleh ubah. Dapatan kajian menunjukkan bahawa tahap ketidaksedaran pelajar adalah pada tahap yang rendah (min 2.517). Bagi pengalaman penipuan, majoriti responden tidak pernah atau hanya segelintir sahaja yang pernah tertipu dalam talian yang berkaitan dengan terpedaya dengan penipuan dalam talian. Mankala analisis regresi linear menunjukkan bahawa terdapat hubungan yang signifikan antara tahap ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dengan pengalaman pelajar yang pernah terkena scam dalam talian. Kajian ini penting kepada institusi mahupun dalam kalangan pensyarah untuk terus mendidik pelajar yang menggunakan sebarang perkhidmatan Wi-Fi atau internet percuma yang boleh membawa kepada risiko.*

Kata kunci: *Wi-Fi Awam, Risiko keselamatan, Ketidaksedaran*

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

Abstract: *The objective of this study is to assess the level of awareness regarding security risks in the use of public Wi-Fi networks and to identify experiences of online scams among students. Additionally, this study aims to examine whether there is a relationship between the lack of awareness of security risks in public Wi-Fi usage and the experience of online scams among students. The study sample consists of students from higher learning institutions. Students were chosen as the sample because many often face financial difficulties and are constrained by the inability to afford data quotas for internet access. This study employs a quantitative approach using a survey method. The sample consists of students from Politeknik Besut Terengganu. The sampling technique used is random sampling. The collected data will be analyzed using descriptive analysis to determine the level of students' awareness of security risks in the use of public Wi-Fi networks. Linear regression analysis will be used to determine the relationship between the variables. The findings indicate that the students' level of unawareness is low (mean 2.517). Regarding scam experiences, the majority of respondents have never fallen victim to or only a few have been deceived by online scams. Meanwhile, the linear regression analysis shows a significant relationship between the level of unawareness of security risks in public Wi-Fi usage and students' experience of falling victim to online scams. This study is important for institutions and lecturers to continue educating students who use any free Wi-Fi or internet services that may pose risks.*

Keywords: *Public Wi-Fi, Security risks, Unawareness*

Pengenalan

Pada masa kini, Wi-Fi awam diletakkan hampir di setiap tempat awam seperti di lapangan terbang, taman hiburan, kedai kopi, pusat membeli-belah dan banyak lagi lokasi lain. Kebanyakan orang lebih suka internet percuma kerana mereka boleh memuat turun sumber seperti filem, menonton video YouTube, Instagram Reels dan kebanyakan aktiviti media sosial tanpa sebarang kos penggunaan data internet mereka (Bheevgade et al., 2022). Walaupun ianya merupakan kemudahan untuk orang ramai, hotspot Wi-Fi awam juga boleh memudahkan pencurian identiti dan penjenayah siber untuk memantau apa yang seseorang lakukan dalam talian dan mencuri kata laluan, maklumat peribadi pengguna Wi-Fi awam atau kedua-duanya. Europol (2020) menegaskan supaya sentiasa berwaspada dan jangan sekali-kali menganggap bahawa rangkaian Wi-Fi awam selamat atau terjamin. Ini kerana kata laluan Wi-Fi awam ini adalah dikongsi, justeru sesiapa sahaja yang berdekatan boleh melayari rangkaian dengan mudah dan melihat apa yang seseorang lakukan (Europol, 2020).

Walaupun Wi-Fi awam menyediakan sambungan rangkaian yang mudah, ia mempunyai kelemahan keselamatan yang ketara (Louw & Von Solms, 2019; Faíscas, 2022; Zulkipli & Khusairi, 2024). Menurut Choi et al. (2022), walaupun kebanyakan orang mempunyai pengetahuan yang luas tentang potensi kelemahan yang terdapat pada Wi-Fi awam, namun kebanyakan mereka tetap menyambungkannya dengan Wi-Fi awam untuk mendapatkan internet percuma. Keadaan ini dilihat sangat membimbangkan kerana mereka terdedah kepada risiko keselamatan data. Antara kumpulan yang mudah untuk menggunakan Wi-Fi awam adalah pelajar. Ini berdasarkan kepada kajian Rahim et al. (2020) yang mendapati sebahagian pelajar menghadapi kekangan kewangan walaupun untuk membeli keperluan asas, justeru sekiranya ada Wi-Fi awam, kemungkinan mereka adalah salah satu pengguna Wi-Fi tersebut tanpa menyedari risiko keselamatan data. Justeru itu, kajian perlu dijalankan untuk melihat tahap ketidaksedaran terhadap risiko keselamatan dan untuk mengenal pasti sama ada mereka

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

mempunyai pengalaman terkena penipuan dalam talian. Kajian ini penting bagi kepada institusi mahupun dalam kalangan pensyarah untuk terus mendidik pelajar yang menggunakan sebarang perkhidmatan Wi-Fi atau internet percuma yang boleh membawa kepada risiko.

Objektif kajian

Kajian ini dijalankan adalah untuk:

a) Mengenal pasti tahap ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dalam kalangan pelajar.
b) Mengenal pasti pengalaman terkena penipuan (scam) dalam kalangan pelajar.
c) Mengenal pasti hubungan antara ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam terhadap pengalaman terkena penipuan (scam) dalam talian dalam kalangan pelajar.

Sorotan kajian

Rangkaian Wi-Fi awam merupakan akses internet percuma dan mempunyai kebaikan kepada kumpulan tertentu yang memerlukan (Hampton & Gupta, 2008; Lambert et al., 2014; Backhouse & Chauke, 2020). Namun begitu ianya mempunyai dilihat kurang selamat, berisiko dan terdedah kepada pelbagai ancaman siber (Sombatruang et al., 2018; Kaleta & Mahadevan, 2020; Sangen et al., 2023). Hotspot Wi-Fi awam selalunya tidak selamat, bermakna sesiapa sahaja di rangkaian yang sama berpotensi melihat data yang dihantar. Rangkaian Wi-Fi awam biasanya lemah atau tiada pengesahan pengguna, menjadikannya sangat tidak selamat. Pengguna yang menggunakan rangkaian Wi-Fi awam umumnya tidak menyedari potensi risiko yang mungkin dihadapi oleh data mereka. Dalam kebanyakan kes, pengguna hanya menyedari maklumat peribadi mereka telah dikompromi apabila sudah terlambat untuk membetulkan keadaan (Sangen et al., 2023). Kajian Bheevgade et al. (2022) menjelaskan bahawa kebanyakan penceroboh menggunakan Wi-Fi awam untuk menjalankan aktiviti jenayah siber dan bagaimana penceroboh boleh mengakses data peribadi seseorang atau memuat turun data mereka dengan mudah kerana mereka telah bersambung melalui rangkaian Wi-Fi awam yang mempunyai niat jahat. Di saping itu, banyak rangkaian Wi-Fi awam tidak disulitkan, menjadikannya mudah untuk perisian *malware* merebak, serangan orang tengah berlaku, dan sambungan dirampas. Akibatnya, mereka membahayakan privasi dan keselamatan pengguna mereka dalam pelbagai cara (Marat, 2023).

Metodologi kajian

Kajian ini merupakan kajian kuantitatif. Sampel kajian adalah pelajar Politeknik Besut Terengganu (PoliBesut). Untuk mendapatkan data, kajian ini menggunakan soal selidik yang diedarkan melalui *Google Form*. Teknik pensampelan yang digunakan adalah pensampelan rawak kerana semua pelajar di PoliBesut mempunyai peluang untuk terlibat dalam kajian ini. Maklum balas responden akan diukur menggunakan 5-skala likert. Data yang dikumpulkan melalui soal selidik *Google Form* akan dianalisis menggunakan perisian *Statistical Package for the Social Sciences* (SPSS). Analisis kajian yang digunakan adalah analisis deskriptif dan regresi linear. Tahap interpretasi min adalah berdasarkan skala yang digunakan oleh Ngadiman et al. (2019) iaitu: 1.00–1.99 (Lemah), 2.00–2.99 (Rendah), 3.00–3.99 (Sederhana), dan 4.00–5.00 (Tinggi). Manakala dalam regresi linear, hubungan antara pemboleh ubah akan ditentukan melalui nilai-p (p-value). P-value yang lebih kecil daripada 0.05 akan dianggap mempunyai hubungan antara pemboleh ubah bebas n dengan pemboleh ubah bersandar.

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

Hasil Kajian

a) Latar belakang responden

Jadual 1: Latar Belakang Responden

Item		n	%
Jantina	Lelaki	30	50.0
	Perempuan	30	50.0
Program	Diploma Reka Bentuk Fesyen Batik	8	13.3
	Diploma Reka Bentuk Kraf	3	5.0
	Diploma Teknologi Maklumat	49	81.7
Semester	2	32	53.3
	3	5	8.3
	4	19	31.7
	5	3	5.0
	Latihan Industri	1	1.7
HPNM	2.01 - 2.99	2	3.3
	3.00 - 3.33	16	26.7
	3.43 - 3.67	18	30.0
	3.68 - 4.00	23	38.3
	Semester 1 (Tiada HPNM)	1	1.7

Jadual 1 menunjukkan latar belakang responden yang terlibat dalam kajian ini yang terdiri daripada pelajar lelaki (50%) dan perempuan (50%). Bagi program pengajian, majoriti responden mengikuti program Diploma Teknologi Maklumat (81.7%), diikuti oleh Diploma Reka Bentuk Fesyen Batik (13.3%) dan Diploma Reka Bentuk Kraf (5.0%). Majoriti responden berada di semester 2 (53.3%), diikuti oleh semester 4 (31.7%). Berdasarkan kepada prestasi akademik yang diukur melalui HPNM, majoriti responden mempunyai prestasi akademik yang baik iaitu HPNM 3.00 – 3.33 (26.7%), 3.43 – 3.67 (30.0%) dan 38.3% responden mempunyai HPNM antara 3.68 – 4.00.

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

b) Mengenal pasti tahap ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dalam kalangan pelajar

Jadual 2: Dapatan Analsis Deskriptif

No	Item	S.P	Mean	Tahap
E1	Tidak sedar bahawa Wi-Fi awam boleh membahayakan keselamatan data peribadi.	1.418	2.583	Rendah
E2	Tidak tahu bahawa serangan "man-in-the-middle" boleh berlaku di Wi-Fi awam.	1.291	2.833	Rendah
E3	Tidak terfikir bahawa penggodam boleh mengakses data melalui Wi-Fi awam.	1.334	2.467	Rendah
E4	Jarang menyedari risiko keselamatan tanpa VPN di Wi-Fi awam.	1.294	2.550	Rendah
E5	Tidak faham pentingnya menyemak keselamatan rangkaian Wi-Fi.	1.223	2.383	Rendah
E6	Kurang sedar bahawa Wi-Fi awam boleh menyebabkan kebocoran maklumat peribadi dan kewangan.	1.279	2.417	Rendah
E7	Sering menggunakan Wi-Fi awam tanpa memikirkan risiko keselamatan.	1.269	2.483	Rendah
E8	Tidak pernah mendengar tentang perisian hasad yang boleh merebak melalui Wi-Fi awam.	1.295	2.483	Rendah
E9	Tidak tahu bahawa sesi log masuk dalam talian boleh dibaca oleh pihak ketiga semasa menggunakan Wi-Fi awam.	1.269	2.517	Rendah
E10	Tidak sedar bahawa menggunakan Wi-Fi awam yang tidak disulitkan boleh menyebabkan kebocoran data sensitif seperti nombor kad kredit.	1.281	2.450	Rendah
	Purata	*1.147*	*2.517*	*Rendah*

Jadual 2 menunjukkan dapatan analisis untuk mengenal pasti tahap ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dalam kalangan pelajar. Item dalam kajian ini adalah bersifat negatif. Secara puratanya, analisis ini menunjukkan bahawa tahap ketidaksedaran pelajar adalah pada tahap yang rendah (min 2.517). Majoriti pelajar mempunyai tahap kesedaran yang baik mengenai risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam. Dapatan ini menjelaskan perlunya meningkatkan tahap kesedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam kerana rangkaian ini sering kali tidak dilindungi dengan sekuriti yang mencukupi, memudahkan penyerang untuk mengakses data sensitif pengguna. Tanpa kesedaran yang tinggi, pengguna mungkin terdedah kepada ancaman seperti pencurian identiti atau serangan siber yang boleh membawa kepada kerugian kewangan atau pendedahan maklumat peribadi

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

c) Mengenal pasti pengalaman terkena penipuan (scam) dalam kalangan pelajar

Jadual 3: Dapatan Analsis Deskriptif

No	Item	S.P	Mean	Tahap
B1	Pernah terpedaya dengan tawaran palsu atau penipuan dalam talian.	1.162	1.850	Lemah
B2	Pernah memberikan maklumat peribadi kepada pihak yang tidak dikenali selepas terpedaya.	0.965	1.517	Lemah
B3	Pernah menjadi mangsa penipuan melalui e-mel atau mesej.	1.071	1.650	Lemah
B4	Pernah kehilangan wang akibat penipuan dalam talian.	1.313	1.733	Lemah
	Purata	*1.013*	*1.688*	*Lemah*

Jadual 3 menunjukkan dapatan analisis deskriptif berkaitan pengalaman pelajar mengenai penipuan (scam) dalam talian. Secara puratanya, min berada pada tahap yang lemah (min 1.688) yang menjelaskan bahawa majoriti responden tidak pernah atau hanya segelintir sahaja yang pernah tertipu dalam talian yang berkaitan dengan terpedaya dengan penipuan dalam talian seperti pernah terpedaya dengan tawaran palsu (min 1.850), pernah memberikan maklumat peribadi kepada pihak yang tidak dikenali (min 1.517) dan pernah menjadi mangsa penipuan melalui e-mel (min 1.650). Kesimpulannya, majoriti pelajar menunjukkan mereka tidak mempunyai pengalaman terjerat dengan penipuan dalam talian. Ini menunjukkan bahawa walaupun penipuan dalam talian wujud, kesedaran dan tindakan berjaga-jaga pelajar telah mengurangkan risiko mereka untuk menjadi mangsa.

d) Mengenal pasti hubungan antara ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam terhadap pengalaman terkena penipuan (scam) dalam talian dalam kalangan pelajar

Jadual 3: Ringkasan Analisis Regresi Linear

Hubungan	S.P	Beta	Nilai-t	Nilai-p	Status
Ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam → Pengalaman terkena scam	0.111	0.278	2.200	0.032	Sig.

Berdasarkan analisis regresi linear yang ditunjukkan dalam Jadual 3, terdapat hubungan yang signifikan antara tahap ketidaksedaran terhadap risiko keselamatan dalam penggunaan rangkaian Wi-Fi awam dengan pengalaman pelajar yang pernah terkena scam dalam talian, di mana ketidaksedaran terhadap risiko keselamatan dalam penggunaan Wi-Fi awam memberi kesan positif terhadap kemungkinan pelajar terdedah kepada scam. Ini menunjukkan bahawa semakin rendah kesedaran pelajar terhadap risiko keselamatan, semakin tinggi kemungkinan mereka mengalami penipuan dalam talian. Secara kesimpulannya, dapatan ini menjelaskan pentingnya meningkatkan kesedaran keselamatan dalam penggunaan rangkaian Wi-Fi awam untuk mengurangkan risiko terkena penipuan dalam talian.

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

Kesimpulan

Wi-Fi awam kini menjadi keperluan penting bagi kumpulan yang memerlukan akses internet, seperti pelajar, pekerja jarak jauh, dan masyarakat yang tinggal di kawasan terpencil. Ia menyediakan kemudahan komunikasi, pendidikan, dan perniagaan tanpa memerlukan kos yang tinggi. Namun, penggunaan rangkaian Wi-Fi awam datang dengan risiko keselamatan yang besar, termasuk pendedahan kepada serangan siber dan pencurian data. Oleh itu, individu perlu lebih berhati-hati dengan maklumat yang mereka kongsi dalam rangkaian ini, manakala kerajaan pula harus mengambil peranan dalam menyediakan peraturan dan infrastruktur keselamatan yang lebih baik untuk melindungi pengguna

Rujukan

Backhouse, J., & Chauke, H. (2020). Development impacts of free public Wi-Fi in Johannesburg. In *Handbook of Research on Managing Information Systems in Developing Economies* (pp. 374-395). IGI Global.

Bheevgade, P., Saha, C., Nath, R., Dabhade, S., Barot, H., & Junare, S. O. (2022, December). The rise of public Wi-Fi and threats. In *International Conference on Information Security, Privacy and Digital Forensics* (pp. 175-189). Singapore: Springer Nature Singapore.

Choi, H. S., Carpenter, D., & Ko, M. S. (2022). Risk taking behaviors using public Wi-fi™. *Information Systems Frontiers*, *24*(3), 965-982.

Europol. (20 Julai 2020). *Risks of using public Wi-Fi*. Europol. Diambil pada 8 April 2026, daripada https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/risks-of-using-public-wi-fi

Faíscas, D. (2022). (In) security in Wi-Fi networks: A systematic review. *ARIS2-Advanced Research on Information Systems Security*, *2*(2), 17-23.

Hampton, K. N., & Gupta, N. (2008). Community and social interaction in the wireless city: wi-fi use in public and semi-public spaces. *New Media & Society*, *10*(6), 831-850.

Kaleta, J. P., & Mahadevan, L. (2020). Examining differences in perceptions of trust, privacy and risk in home and public Wi-Fi internet channels. *Journal of systems and information technology*, *22*(3), 265-287.

Lambert, A., McQuire, S., & Papastergiadis, N. (2014). Public Wi-Fi: Space, sociality and the social good. *Journal of Telecommunications and the Digital Economy*, *2*(3), 45-1.

Louw, C., & Von Solms, B. (2019). Free public Wi-Fi security in a smart city context—an end user perspective. In *Smart Cities Cybersecurity and Privacy* (pp. 113-127). Elsevier.

Marat, A. (2023). *Risks of using public Wi-Fi. International Journal of Innovative Science and Research Technology, 8*(9).

Ngadiman, D. W. T., Yacoob, S. E., & Wahid, H. (2019). Tahap Harga Diri Kumpulan Berpendapatan Rendah yang Berhutang dan Peranan Organisasi dalam Sektor Perladangan. *Melayu: Jurnal Antarabangsa Dunia Melayu*, *12*(2), 238-254.

Rahim, H. A., Seng, N. D., Ngadiman, D. W. T., & Ismail, N. A. (2020). The debt management patterns of educational loan recipients among Polytechnic Students In Kota Kinabalu, Sabah: An Empirical Study. *International Journal of Accounting*, *5*(28), 49-57.

Sangeen, M., Bhatti, N. A., Kifayat, K., Alsadhan, A. A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. *Computer Communications*, *209*, 359-367.

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018, August). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In *2018 16th annual conference on Privacy, Security and Trust (PST)* (pp. 1-11). IEEE.

Volume: 9 Issues: 29 [March, 2026] pp. 41 - 48]
Jurnal Penyelidikan Sains Sosial (JOSSR)
eISSN: 2637 -0956
Journal Website: https://academicinspired.com/jossr
DOI: 10.55573/JOSSR.092906

Zulkipli, N. H. N., & Khusairi, M. I. B. (2024, August). An experimental analysis for public Wi-Fi attacks. In *2024 IEEE 6th Symposium on Computers & Informatics (ISCI)* (pp. 247-252). IEEE.