Jurnal Teknik Informatika dan Teknologi Informasi
Volume 6, Nomor 2, Agustus 2026
e-ISSN: 2827-9387, p-ISSN: 2827-9379, Hal. 399-412
DOI: https://doi.org/10.55606/jutiti.v6i2.7568
Tersedia: https://journalshub.org/index.php/jutiti

Analisis Tingkat Kesadaran Keamanan Siber Mahasiswa STMIK Pesat Nabire Provinsi Papua Tengah terhadap Ancaman *Phishing* dan *Malware*

Murtiningsih Yunus[1*], Marselino Marthen Yogi[2], Erik Oktavianus Allo[3], Marco Yeri Maswatu[4], Eka Ardhianto[5], Aji Supriyanto[6]
[1-6]Program Studi Teknologi Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank, Semarang, Indonesia
Email: murtiningsihyunus0032@mhs.unisbank.ac.id[1], marselinomarthen0034@mhs.unisbank.ac.id[2], erikoktavianus0038@mhs.unisbank.ac.id[3], marcoyeri0036@mhs.unisbank.ac.id[4], ekaardhianto@edu.unisbank.ac.id[5], ajisup@edu.unisbank.ac.id[6]
**Penulis Korespondensi: murtiningsihyunus0032@mhs.unisbank.ac.id*

Abstract*. The expansion of digital services in higher education has increased students' dependence on the internet for accessing academic information, communicating, storing data, and using application-based services. These benefits are accompanied by higher exposure to phishing and malware threats. This study analyzes the cybersecurity awareness level of STMIK Pesat Nabire students in Central Papua Province toward phishing and malware threats using pre-test and post-test measurements. A quantitative approach with a pre-experimental one-group pre-test and post-test design was applied. The instrument consisted of 15 Likert-scale items grouped into three dimensions: phishing threat awareness, malware threat awareness, and user self-protection behavior. Based on participant-name and student-number matching between the pre-test and post-test sheets, 120 respondents had complete paired data. The findings show that the mean cybersecurity awareness score increased from 2.83 in the pre-test to 3.89 in the post-test. The increase was statistically significant at the 5 percent level (t = 22.241; p < 0.001), with a strong effect size (Cohen's dz = 2.03). The largest improvement occurred in the malware threat dimension, followed by phishing threat awareness and user self-protection behavior. These findings indicate that practical cybersecurity education can strengthen students' awareness, particularly in recognizing unsafe software, suspicious links, and secure account practices. However, self-protection practices such as MFA/2FA, VPN use, and password manager adoption require continuous reinforcement.*

Keywords*: Cybersecurity; Cybersecurity Awareness; Malware; Phishing; University Students.*

Abstrak. Perkembangan layanan digital di perguruan tinggi membuat mahasiswa semakin bergantung pada internet untuk mengakses informasi akademik, berkomunikasi, menyimpan data, dan menggunakan berbagai layanan berbasis aplikasi. Ketergantungan tersebut memberi kemudahan, tetapi juga meningkatkan risiko paparan terhadap phishing dan malware. Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan siber mahasiswa STMIK Pesat Nabire Provinsi Papua Tengah terhadap ancaman phishing dan malware melalui pengukuran pre-test dan post-test. Penelitian menggunakan pendekatan kuantitatif dengan desain pre-eksperimental one-group pre-test and post-test. Instrumen terdiri atas 15 butir pernyataan skala Likert 1-5 yang dikelompokkan ke dalam tiga dimensi, yaitu ancaman phishing, ancaman malware, dan pertahanan mandiri pengguna. Berdasarkan pemadanan nama dan NIM pada lembar pre-test dan post-test, diperoleh 120 responden dengan data lengkap. Hasil penelitian menunjukkan bahwa rerata kesadaran keamanan siber meningkat dari 2,83 pada pre-test menjadi 3,89 pada post-test. Peningkatan tersebut signifikan secara statistik pada taraf 5 persen (t = 22,241; p < 0,001) dengan ukuran efek yang kuat (Cohen's dz = 2,03). Peningkatan terbesar terjadi pada dimensi ancaman malware, diikuti ancaman phishing dan pertahanan mandiri pengguna. Temuan ini menunjukkan bahwa edukasi keamanan siber berbasis contoh praktis mampu memperkuat kesadaran mahasiswa, terutama dalam mengenali risiko perangkat lunak tidak aman, tautan mencurigakan, dan kebiasaan perlindungan akun. Meskipun demikian, aspek pertahanan mandiri seperti penggunaan MFA/2FA, VPN, dan password manager masih perlu diperkuat secara berkelanjutan

Kata Kunci: Keamanan Siber; Kesadaran Keamanan Siber; Mahasiswa; *Malware*; *Phishing*.

Naskah Masuk: 30 April 2026; Revisi: 04 Juni 2026; Diterima: 10 Juli 2026; Tersedia: 24 Juli 2026

1. LATAR BELAKANG

Transformasi digital di lingkungan perguruan tinggi telah mengubah aktivitas akademik menjadi sangat bergantung pada jaringan internet. Integrasi sistem informasi akademik, platform pembelajaran daring, dan manajemen dokumen digital meningkatkan efisiensi layanan bagi sivitas akademika. Namun, interkoneksi tersebut juga memperluas kerentanan serta titik masuk risiko keamanan siber. Studi pada lingkungan pendidikan tinggi menunjukkan bahwa pertumbuhan layanan digital perlu diimbangi dengan penguatan perilaku keamanan dan budaya kesadaran siber karena mahasiswa berinteraksi intensif dengan berbagai layanan daring dan aset informasi kampus (Bognár & Bottyán, 2024; Armas & Taherdoost, 2025).

Di antara berbagai ancaman digital, phishing dan malware menjadi risiko yang dekat dengan aktivitas mahasiswa. Serangan phishing memanfaatkan rekayasa sosial melalui surat elektronik, pesan instan, situs tiruan, tautan, dan media digital lain untuk memperoleh informasi sensitif. Sementara itu, malware berkembang melalui perangkat lunak berbahaya dan berbagai teknik penyamaran yang dapat mengganggu kerahasiaan, integritas, serta ketersediaan data. Kajian sistematis menunjukkan bahwa keberhasilan mitigasi phishing tidak cukup mengandalkan kontrol teknis karena kemampuan pengguna mengenali manipulasi dan mengambil keputusan aman tetap menentukan, sedangkan ancaman malware terus berkembang mengikuti perubahan platform dan teknik pengelabuan (Naqvi et al., 2023; Varshney et al., 2024).

Sebagai institusi pendidikan tinggi berbasis teknologi informasi, mahasiswa STMIK Pesat Nabire memiliki intensitas interaksi digital yang tinggi sehingga relevan dikaji dalam konteks ancaman siber. Latar belakang akademik di bidang teknologi tidak serta-merta menjamin konsistensi perilaku keamanan digital. Pengabaian autentikasi berlapis, penundaan pembaruan perangkat lunak, penggunaan kata sandi yang lemah, dan kebiasaan membuka tautan tanpa verifikasi dapat tetap terjadi pada pengguna yang aktif secara digital. Penelitian terdahulu menunjukkan bahwa kesadaran keamanan siber mahasiswa dipengaruhi oleh pengetahuan, sikap, perilaku keamanan, persepsi kemampuan diri, dan pengalaman pelatihan (Ahamed et al., 2024; Alharbi & Tassaddiq, 2021; Alqahtani, 2022).

Di Indonesia, kajian mengenai perilaku dan kesadaran keamanan siber mahasiswa mulai berkembang. Sejumlah penelitian telah membahas hubungan pengetahuan, sikap, perilaku, dan pelatihan dengan kesadaran siber (Fattah et al., 2023), integrasi Protection Motivation Theory dan Theory of Planned Behavior untuk menjelaskan perilaku keamanan mahasiswa (Gustara et al., 2025), serta pengukuran kesadaran keamanan informasi pada

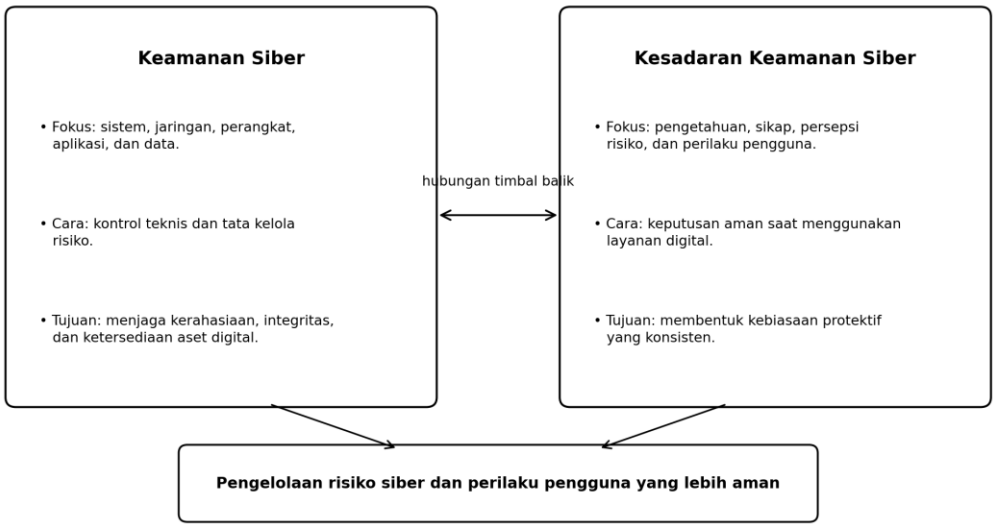
mahasiswa perguruan tinggi (Perkasa et al., 2024). Namun, penelitian yang menempatkan Papua Tengah, khususnya STMIK Pesat Nabire, sebagai konteks utama masih terbatas. Kesenjangan ini penting dikaji karena instrumen kesadaran keamanan perlu mempertimbangkan karakteristik pengguna, pola interaksi digital, dan konteks pendidikan tempat perilaku keamanan dibentuk (Rohan et al., 2025).

Guna mengisi celah riset tersebut, penelitian ini bertujuan menganalisis tingkat kesadaran keamanan siber mahasiswa STMIK Pesat Nabire terhadap ancaman phishing dan malware. Secara khusus, penelitian ini diarahkan untuk: (1) memetakan kondisi awal kesadaran keamanan siber mahasiswa, (2) mengukur perubahan skor kesadaran melalui pre-test dan post-test pada 120 responden yang sama, dan (3) mengidentifikasi aspek pertahanan mandiri yang masih memerlukan penguatan. Hasil penelitian diharapkan memberikan bukti empiris dan dasar praktis bagi kampus untuk menyusun program literasi keamanan digital yang sesuai dengan kebutuhan mahasiswa.

2. KAJIAN TEORITIS

Keamanan siber merupakan upaya sistematis untuk melindungi sistem, jaringan, perangkat, aplikasi, dan data dari akses tidak sah, gangguan, perubahan, maupun kerusakan. Pada tingkat individu, efektivitas perlindungan tidak hanya ditentukan oleh kontrol teknis, tetapi juga oleh keputusan pengguna ketika berinteraksi dengan layanan digital. Kesadaran keamanan siber merujuk pada kemampuan individu mengenali risiko, memahami konsekuensi ancaman, menilai situasi digital, dan menerapkan tindakan pencegahan secara konsisten. Dengan demikian, keamanan siber berorientasi pada perlindungan aset dan pengelolaan risiko, sedangkan kesadaran keamanan siber berorientasi pada pengetahuan, sikap, persepsi risiko, dan perilaku pengguna yang mendukung perlindungan tersebut (Bognár & Bottyán, 2024; Armas & Taherdoost, 2025).

Dalam lingkungan pendidikan tinggi, pemetaan kesadaran keamanan siber perlu mempertimbangkan karakteristik pengguna, intensitas penggunaan layanan digital, dan kebiasaan perlindungan akun. Mahasiswa dapat memiliki tingkat pemahaman dan perilaku keamanan yang berbeda meskipun berada dalam lingkungan akademik yang sama. Karena itu, instrumen pengukuran perlu disesuaikan dengan pengalaman digital mahasiswa agar mampu menangkap perilaku nyata, bukan hanya pengetahuan definisional (Bognár & Bottyán, 2024; Rohan et al., 2025). Berdasarkan pertimbangan tersebut, penelitian ini menggunakan tiga dimensi yang dekat dengan aktivitas mahasiswa, yaitu ancaman phishing, ancaman malware, dan pertahanan mandiri pengguna.



Gambar 1. Skema perbedaan keamanan siber dan kesadaran keamanan siber.

Sumber: sintesis peneliti berdasarkan Bognár dan Bottyán (2024) serta Armas dan Taherdoost (2025).

3. METODE PENELITIAN

Penelitian dilakukan melalui rangkaian tahap yang dimulai dari identifikasi masalah dan kajian literatur, penyusunan instrumen, pelaksanaan pre-test, penguatan materi keamanan siber, pelaksanaan post-test, pemadanan data responden, pengujian instrumen, analisis statistik, dan interpretasi hasil. Urutan tersebut digunakan agar proses pengumpulan dan pengolahan data dapat dijelaskan secara sistematis dari tahap awal sampai penyusunan rekomendasi.

Jenis dan Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain pre-eksperimental one-group pre-test and post-test. Desain ini digunakan untuk membandingkan tingkat kesadaran keamanan siber pada kelompok responden yang sama sebelum dan setelah edukasi atau penguatan materi. Analisis diarahkan pada perubahan skor rata-rata, distribusi kategori, validitas, reliabilitas, serta dimensi yang masih membutuhkan penguatan. Karena data pre-test dan post-test berasal dari responden yang sama, uji beda dilakukan dengan pendekatan berpasangan (Kim, 2015).

Desain penelitian tidak menggunakan kelompok kontrol. Oleh karena itu, hasil penelitian ditafsirkan sebagai bukti empiris mengenai perubahan skor dalam kelompok mahasiswa yang sama, bukan sebagai pembuktian kausalitas mutlak. Pembatasan interpretasi ini penting agar perubahan skor tidak secara langsung diklaim hanya disebabkan oleh satu faktor di luar desain penelitian.

Instrumen Penelitian

Instrumen penelitian berupa kuesioner skala *Likert* lima tingkat, yaitu 1 = sangat tidak setuju, 2 = tidak setuju, 3 = netral, 4 = setuju, dan 5 = sangat setuju. Instrumen terdiri atas 15 pernyataan yang dibagi ke dalam tiga dimensi: ancaman *phishing* (AP1-AP5), ancaman *malware* (AM1-AM5), dan pertahanan mandiri pengguna (PM1-PM5). Skor dimensi dihitung dari rerata lima butir pada setiap dimensi, sedangkan skor total dihitung dari rerata seluruh butir. Penggunaan skala *Likert* lazim dipakai untuk membaca kecenderungan sikap dan persepsi responden secara bertingkat (Boone & Boone, 2012; Sullivan & Artino, 2013).

Penyusunan indikator merujuk pada isu keamanan siber yang dekat dengan aktivitas mahasiswa, seperti pemeriksaan alamat email dan URL, kewaspadaan terhadap tautan singkat, penggunaan perangkat lunak legal, pembaruan sistem, pemindaian flashdisk, penggunaan kata sandi kuat, aktivasi MFA/2FA, dan penggunaan password manager. Indikator tersebut diselaraskan dengan penelitian kesadaran keamanan siber mahasiswa dan perilaku keamanan informasi di perguruan tinggi (Ahamed et al., 2024; Alharbi & Tassaddiq, 2021; Bognár & Bottyán, 2024; Rohan et al., 2025).

Tabel 1. Kisi-kisi Instrumen Penelitian.

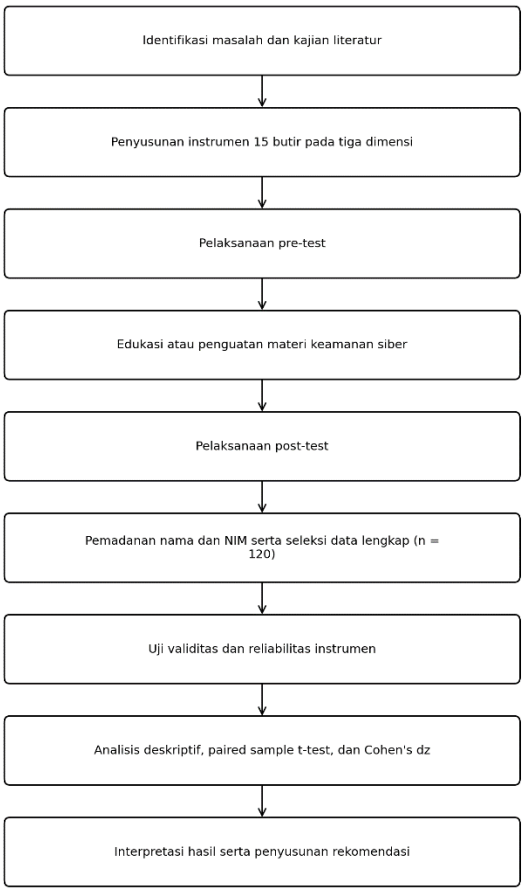
Kode	Dimensi	Indikator ringkas
AP1	Ancaman *phishing*	Memeriksa kecocokan alamat *email* pengirim
AP2	Ancaman *phishing*	Memverifikasi informasi hadiah/bantuan melalui situs resmi
AP3	Ancaman *phishing*	Memeriksa *URL* dan *HTTPS* sebelum *login*
AP4	Ancaman *phishing*	Mengabaikan pesan darurat yang meminta data pribadi
AP5	Ancaman *phishing*	Memeriksa tujuan tautan singkat sebelum diklik
AM1	Ancaman *malware*	Menggunakan perangkat lunak asli atau *open-source*
AM2	Ancaman *malware*	Memperbarui sistem operasi dan antivirus
AM3	Ancaman *malware*	Memastikan antivirus aktif saat instalasi aplikasi
AM4	Ancaman *malware*	Memindai flashdisk/perangkat penyimpanan luar
AM5	Ancaman *malware*	Mengidentifikasi *file* berbahaya berekstensi ganda
PM1	Pertahanan mandiri pengguna	Menggunakan kata sandi berbeda dan kompleks
PM2	Pertahanan mandiri pengguna	Mengaktifkan *MFA/2FA* pada akun utama
PM3	Pertahanan mandiri pengguna	Menggunakan data pribadi/*VPN* saat transaksi umum
PM4	Pertahanan mandiri pengguna	Mengganti sandi dan memeriksa *log* saat akun mencurigakan
PM5	Pertahanan mandiri pengguna	Menggunakan *password manager*

Sumber: rancangan instrumen penelitian, 2026.

Prosedur Penelitian

Tahap penelitian dimulai dengan identifikasi masalah kesadaran keamanan siber mahasiswa dan kajian literatur untuk menentukan dimensi pengukuran. Selanjutnya, instrumen 15 butir disusun pada tiga dimensi, yaitu ancaman phishing, ancaman malware, dan pertahanan mandiri. Responden mengisi pre-test untuk memperoleh gambaran kondisi awal. Setelah itu, mahasiswa memperoleh edukasi atau penguatan materi keamanan siber yang membahas contoh ancaman dan tindakan perlindungan sesuai tiga dimensi instrumen, kemudian mengisi post-test.

Data pre-test dan post-test dipadankan menggunakan nama dan NIM sebagai kunci pencocokan internal. Hanya responden dengan pasangan data lengkap yang digunakan sehingga diperoleh 120 data berpasangan. Tahap berikutnya meliputi uji validitas, uji reliabilitas, analisis deskriptif, paired sample t-test, perhitungan Cohen's dz, serta interpretasi dimensi dan butir yang masih memerlukan penguatan. Alur penelitian disajikan pada Gambar 2.



Gambar 2. Alur penelitian.

Sumber: rancangan penelitian, 2026.

4. HASIL DAN PEMBAHASAN

Penelitian dilaksanakan pada mahasiswa STMIK Pesat Nabire Provinsi Papua Tengah. Populasi penelitian adalah mahasiswa aktif yang menggunakan layanan digital dalam aktivitas akademik dan komunikasi sehari-hari. Data penelitian diperoleh dari *file* kuesioner terbaru yang terdiri atas dua lembar, yaitu *PRE-TEST* dan POS-TEST.

Pemadanan data dilakukan berdasarkan kesesuaian nama dan NIM pada lembar *pre-test* dan *post-test*. Berdasarkan proses tersebut, diperoleh 120 responden yang memiliki data lengkap dan dapat dianalisis secara berpasangan. Identitas responden tidak ditampilkan dalam artikel untuk menjaga kerahasiaan data pribadi. Nama dan NIM hanya digunakan sebagai kunci pencocokan internal agar skor *pre-test* dan *post-test* berasal dari responden yang sama.

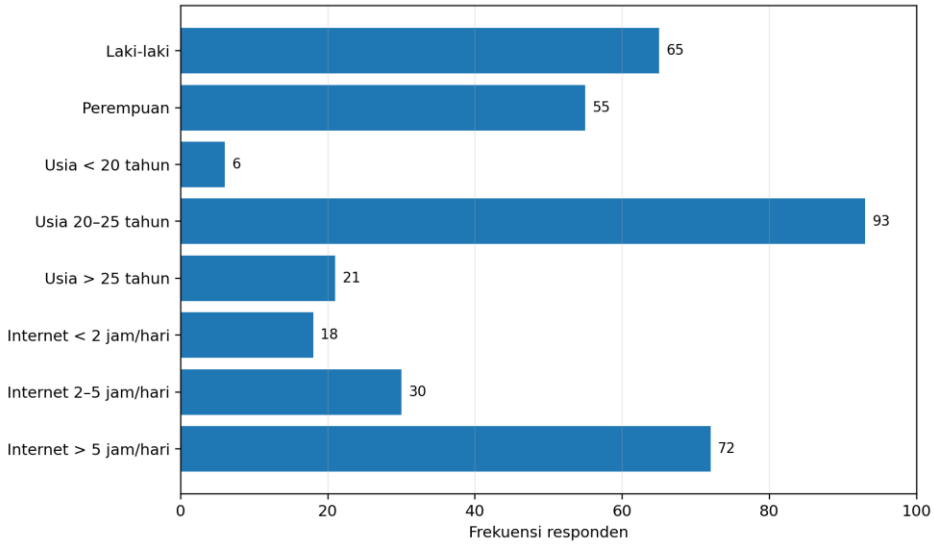
Karakteristik Responden

Jumlah responden yang dapat dianalisis secara berpasangan adalah 120 mahasiswa. Komposisi responden menunjukkan bahwa laki-laki berjumlah 65 orang atau 54,17 persen, sedangkan perempuan berjumlah 55 orang atau 45,83 persen. Sebagian besar responden berada pada rentang usia 20-25 tahun, yaitu 93 orang atau 77,50 persen. Dari sisi intensitas penggunaan internet, mayoritas responden menggunakan internet lebih dari lima jam per hari, yaitu 72 orang atau 60,00 persen. Kondisi ini menunjukkan bahwa responden merupakan pengguna internet aktif sehingga relevan untuk dikaji dalam konteks risiko *phishing* dan *malware*, karena penggunaan layanan digital yang intensif dapat memperbesar peluang berinteraksi dengan pesan, tautan, dan *file* yang tidak aman (Perkasa et al., 2024; Rohan et al., 2025).

Tabel 2. Karakteristik Responden.

Karakteristik	Kategori	Frekuensi	Persentase (%)
Jenis kelamin	LAKI-LAKI	65	54,17
Jenis kelamin	PEREMPUAN	55	45,83
Usia	< 20 Tahun	6	5,00
Usia	20 - 25 Tahun	93	77,50
Usia	> 25 Tahun	21	17,50
Intensitas penggunaan internet per hari	< 2 Jam	18	15,00
Intensitas penggunaan internet per hari	2 - 5 Jam	30	25,00
Intensitas penggunaan internet per hari	> 5 Jam	72	60,00

Sumber: hasil olah data kuesioner, 2026.



Gambar 3. Distribusi karakteristik responden.

Sumber: hasil olah data kuesioner, 2026.

Uji Validitas Instrumen

Hasil uji validitas menunjukkan bahwa seluruh butir pada dimensi ancaman phishing, ancaman malware, dan pertahanan mandiri memiliki nilai r hitung lebih besar dari r tabel 0,179 serta $p < 0,05$. Perhitungan korelasi butir-total mengacu pada Persamaan (3). Dengan demikian, seluruh butir kuesioner dinyatakan valid dan dapat digunakan dalam analisis lanjutan. Hasil ini menunjukkan bahwa setiap butir memiliki hubungan yang memadai dengan skor total dimensi yang diukurnya (Taherdoost, 2016).

Tabel 3. Hasil Uji Validitas Butir.

Kode	Dimensi	r hitung	p	Keterangan
AP1	Ancaman *phishing*	0,646	< 0,001	Valid
AP2	Ancaman *phishing*	0,534	< 0,001	Valid
AP3	Ancaman *phishing*	0,590	< 0,001	Valid
AP4	Ancaman *phishing*	0,608	< 0,001	Valid
AP5	Ancaman *phishing*	0,587	< 0,001	Valid
AM1	Ancaman *malware*	0,611	< 0,001	Valid
AM2	Ancaman *malware*	0,457	< 0,001	Valid
AM3	Ancaman *malware*	0,530	< 0,001	Valid
AM4	Ancaman *malware*	0,560	< 0,001	Valid
AM5	Ancaman *malware*	0,582	< 0,001	Valid
PM1	Pertahanan mandiri	0,620	< 0,001	Valid
PM2	Pertahanan mandiri	0,587	< 0,001	Valid
PM3	Pertahanan mandiri	0,483	< 0,001	Valid
PM4	Pertahanan mandiri	0,659	< 0,001	Valid
PM5	Pertahanan mandiri	0,661	< 0,001	Valid

Sumber: hasil olah data kuesioner, 2026.

Uji Reliabilitas Instrumen

Reliabilitas instrumen dihitung menggunakan Cronbach's Alpha dengan mengacu pada Persamaan (4). Nilai alpha diperoleh dari perbandingan jumlah varians setiap butir ($\Sigma\sigma_i^2$)

terhadap varians skor total (σ_t^2), kemudian dikoreksi berdasarkan jumlah butir (k). Penerapan Persamaan (4) pada matriks skor 15 butir menghasilkan $\alpha = 0{,}781$ untuk pre-test, $\alpha = 0{,}469$ untuk post-test, dan $\alpha = 0{,}893$ untuk data gabungan pre-test dan post-test. Nilai pre-test menunjukkan konsistensi internal yang baik, sedangkan nilai gabungan menunjukkan konsistensi sangat baik. Nilai post-test yang lebih rendah perlu ditafsirkan secara hati-hati karena jawaban cenderung terkonsentrasi pada kategori setuju dan sangat setuju sehingga variasi antarresponden serta kovarians antarbutir menjadi lebih sempit. Kondisi tersebut dapat menurunkan nilai alpha (Tavakol & Dennick, 2011).

Tabel 4. Hasil Uji Reliabilitas Instrumen.

Instrumen/Dimensi	Jumlah butir	*Cronbach's Alpha*	Interpretasi
Pre-test keseluruhan	15	0,781	Reliabel/baik
Post-test keseluruhan	15	0,469	Rendah; ditafsirkan hati-hati
Gabungan *pre-test* dan *post-test*	15	0,893	Sangat baik
Ancaman *phishing* (gabungan)	5	0,784	Baik
Ancaman *malware* (gabungan)	5	0,758	Baik
Pertahanan mandiri (gabungan)	5	0,662	Cukup

Sumber: hasil olah data kuesioner, 2026.

Tingkat Kesadaran Keamanan Siber *Pre-Test* dan *Post-Test*

Rerata skor total kesadaran keamanan siber meningkat dari 2,83 pada pre-test menjadi 3,89 pada post-test. Berdasarkan kategori interpretasi, skor pre-test berada pada kategori sedang, sedangkan skor post-test berada pada kategori tinggi. Hasil paired sample t-test yang dihitung berdasarkan Persamaan (5) menunjukkan perbedaan yang signifikan pada taraf 5 persen ($t = 22{,}241$; $p < 0{,}001$). Ukuran efek Cohen's dz berdasarkan Persamaan (6) sebesar 2,03 menunjukkan perubahan yang besar. Karena data berasal dari responden yang sama, uji t berpasangan sesuai untuk menilai perbedaan skor sebelum dan sesudah pengukuran (Kim, 2015).

Jika dilihat berdasarkan dimensi, peningkatan terbesar terdapat pada ancaman malware, yaitu dari 2,68 menjadi 3,93 dengan selisih 1,25. Dimensi phishing meningkat dari 2,82 menjadi 3,98 dengan selisih 1,16, sedangkan pertahanan mandiri meningkat dari 2,97 menjadi 3,74 dengan selisih 0,77. Ketiga dimensi menunjukkan perubahan yang signifikan. Temuan ini menunjukkan adanya peningkatan kesadaran pada kelompok mahasiswa yang sama setelah rangkaian edukasi dan pengukuran, tanpa menafsirkan hasil sebagai bukti kausal mutlak karena penelitian tidak menggunakan kelompok kontrol.

Tabel 5. Tingkat Kesadaran Keamanan Siber *Pre-Test* dan *Post-Test*.

Dimensi	Mean pre	SD pre	Kategori pre	Mean post	SD post	Kategori post	Selisih	t	p	dz
Total kesadaran keamanan siber	2,83	0,51	Sedang	3,89	0,26	Tinggi	1,06	22,241	< 0,001	2,03
Ancaman *phishing* (AP)	2,82	0,59	Sedang	3,98	0,37	Tinggi	1,16	20,356	< 0,001	1,86
Ancaman *malware* (AM)	2,68	0,58	Sedang	3,93	0,44	Tinggi	1,25	20,647	< 0,001	1,88
Pertahanan mandiri (PM)	2,97	0,63	Sedang	3,74	0,36	Tinggi	0,77	13,479	< 0,001	1,23

Catatan: uji t berpasangan dilakukan pada n = 120. Selisih dihitung dari skor post-test dikurangi skor pre-test.

Distribusi Kategori Kesadaran Keamanan Siber

Distribusi kategori memperlihatkan perubahan yang kuat. Pada *pre-test*, sebagian besar responden berada pada kategori sedang, yaitu 96 orang atau 80,00 persen. Setelah *post-test*, tidak ada lagi responden yang berada pada kategori sangat rendah, rendah, maupun sedang. Sebanyak 109 responden atau 90,83 persen berada pada kategori tinggi dan 11 responden atau 9,17 persen berada pada kategori sangat tinggi. Pola ini memperlihatkan bahwa peningkatan skor tidak hanya terjadi pada nilai rata-rata, tetapi juga terlihat pada perpindahan kategori kesadaran secara umum.

Tabel 6. Distribusi Kategori Kesadaran Keamanan Siber.

Kategori	*Pre-test* f	*Pre-test* %	*Post-test* f	*Post-test* %
Sangat rendah	7	5,83	0	0,00
Rendah	13	10,83	0	0,00
Sedang	96	80,00	0	0,00
Tinggi	4	3,33	109	90,83
Sangat tinggi	0	0,00	11	9,17

Sumber: hasil olah data kuesioner, 2026.

Analisis Per Butir Pernyataan

Walaupun seluruh indikator meningkat, beberapa aspek pertahanan mandiri masih memiliki skor post-test yang relatif lebih rendah dibandingkan indikator lain. PM2 mengenai aktivasi MFA/2FA memiliki rerata post-test 3,52 dan PM3 mengenai penggunaan koneksi data pribadi atau VPN saat transaksi di tempat umum memiliki rerata 3,59. Kedua indikator ini perlu mendapat perhatian karena perlindungan akun dan kebiasaan keamanan daring memerlukan pengetahuan sekaligus praktik yang konsisten (Ahamed et al., 2024; Ahmead et al., 2024; Bognár & Bottyán, 2024; Nagari, 2025).

Tabel 7. Analisis Per Butir Pernyataan.

Kode	Indikator ringkas	Mean pre	Mean post	Selisih	t	p
AP1	Memeriksa kecocokan alamat *email* pengirim	2,94	3,90	0,96	10,170	< 0,001
AP2	Memverifikasi informasi hadiah/bantuan melalui situs resmi	3,12	4,30	1,18	10,920	< 0,001
AP3	Memeriksa *URL* dan *HTTPS* sebelum *login*	2,93	3,98	1,04	9,941	< 0,001
AP4	Mengabaikan pesan darurat yang meminta data pribadi	2,66	3,96	1,30	12,982	< 0,001
AP5	Memeriksa tujuan tautan singkat sebelum diklik	2,44	3,78	1,34	13,502	< 0,001
AM1	Menggunakan perangkat lunak asli atau *open-source*	2,32	3,85	1,53	14,142	< 0,001
AM2	Memperbarui sistem operasi dan antivirus	2,92	3,88	0,96	10,091	< 0,001
AM3	Memastikan antivirus aktif saat instalasi aplikasi	2,80	4,05	1,25	11,244	< 0,001
AM4	Memindai flashdisk/perangkat penyimpanan luar	2,62	3,97	1,34	12,715	< 0,001
AM5	Mengidentifikasi *file* berbahaya berekstensi ganda	2,75	3,92	1,17	11,068	< 0,001
PM1	Menggunakan kata sandi berbeda dan kompleks	3,29	3,99	0,70	7,476	< 0,001
PM2	Mengaktifkan *MFA/2FA* pada akun utama	2,64	3,52	0,88	9,870	< 0,001
PM3	Menggunakan data pribadi/*VPN* saat transaksi umum	2,77	3,59	0,82	9,102	< 0,001
PM4	Mengganti sandi dan memeriksa *log* saat akun mencurigakan	3,06	3,79	0,73	8,453	< 0,001
PM5	Menggunakan *password manager*	3,11	3,81	0,70	8,156	< 0,001

Sumber: hasil olah data kuesioner, 2026.

5. KESIMPULAN DAN SARAN

Penelitian terhadap 120 mahasiswa STMIK Pesat Nabire menghasilkan tiga temuan yang sesuai dengan tujuan penelitian. Pertama, kondisi awal kesadaran keamanan siber berada pada kategori sedang dengan rerata pre-test 2,83. Kedua, skor kesadaran meningkat menjadi 3,89 pada post-test dan masuk kategori tinggi; paired sample t-test menunjukkan perbedaan yang signifikan ($t = 22{,}241$; $p < 0{,}001$) dengan Cohen's $dz = 2{,}03$. Peningkatan terbesar terjadi pada dimensi ancaman malware, diikuti phishing dan pertahanan mandiri. Ketiga, aspek yang masih memerlukan penguatan terutama aktivasi MFA/2FA, penggunaan koneksi yang lebih aman saat transaksi, dan penggunaan password manager. Dengan desain satu kelompok tanpa kontrol, hasil ini menunjukkan perubahan skor pada responden yang sama dan tidak ditafsirkan sebagai bukti kausal mutlak. Temuan tersebut memberi dasar empiris bagi STMIK Pesat Nabire untuk menyusun edukasi keamanan siber yang lebih praktis dan berkelanjutan.

DAFTAR REFERENSI

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Al Fahad, A., Chowdhury, S., & Dey, M. R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. *SAGE Open, 14*(1), 21582440241228920. https://doi.org/10.1177/21582440241228920

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross-sectional study. *Crime Science, 13*, 29. https://doi.org/10.1186/s40163-024-00230-w

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23. https://doi.org/10.3390/bdcc5020023

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://doi.org/10.3390/app12052589

Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information, 16*(5), 336. https://doi.org/10.3390/info16050336

Berrios, S., Leiva, D., Olivares, B., Allende-Cid, H., & Hermosilla, P. (2025). Systematic review: Malware detection and classification in cybersecurity. *Applied Sciences, 15*(14), 7747. https://doi.org/10.3390/app15147747

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588. https://doi.org/10.3390/educsci14060588

Boone, H. N., Jr., & Boone, D. A. (2012). Analyzing Likert data. *Journal of Extension, 50*(2), 1-5. https://doi.org/10.34068/joe.50.02.48

Du, X., & Chintakovid, T. (2023). A survey of cybersecurity awareness among undergraduate students at Yunnan University of Finance and Economics in China. In *Proceedings of*

the International Conference on Educational Technology and Management Science. Atlantis Press. https://www.atlantis-press.com/article/125988338

Eliza, F., Syamsuar, D., & Dwiyanto, F. A. (2024). Assessing student readiness for mobile learning from a cybersecurity perspective. *Online Journal of Communication and Media Technologies, 14*(4), e202451. https://doi.org/10.30935/ojcmt/15017

Fattah, A., Wagimin, & Nurlia. (2023). Enhancing cybersecurity awareness among university students: A study on the relationship between knowledge, attitude, behavior, and training. *JSI: Jurnal Sistem Informasi, 15*(1), 3139-3149. https://doi.org/10.36706/jsi.v15i1.21812

Gustara, M., Cahyadi, E. R., & Sartono, B. (2025). Analysis of cybersecurity awareness and behavior among students of IPB University: An integration of protection motivation theory and theory of planned behavior. *Indonesian Interdisciplinary Journal of Sharia Economics, 8*(3), 13552-13565. https://doi.org/10.31538/iijse.v8i3.8460

Kim, T. K. (2015). T test as a parametric statistic. *Korean Journal of Anesthesiology*, *68*(6), 540-546. https://doi.org/10.4097/kjae.2015.68.6.540

Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2024). A systematic literature review on Windows malware detection: Techniques, research issues, and future directions. *Journal of Systems and Software, 209*, 111921. https://doi.org/10.1016/j.jss.2023.111921

Nagari, S. F. (2025). Cyber security awareness, knowledge and behavior of digital banking users. *Asian Pacific Fraud Journal, 10*(1). https://apfjournal.or.id/index.php/apf/article/view/398

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security, 132*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Perkasa, D. A., Kurniawan, R., & Putra, A. M. (2024). Measuring information security awareness level of higher education students. *MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4*(4). https://journal.irpi.or.id/index.php/malcom/article/view/1461

Rohan, R., Funilkul, S., Chutimaskul, W., Kanthamanon, P., Papasratorn, B., & Pal, D. (2025). Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. *Education and Information Technologies*. https://doi.org/10.1007/s10639-024-13307-5

Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-based phishing detection and student cybersecurity awareness in the digital age. *Big Data and Cognitive Computing*, *9*(8), 210. https://doi.org/10.3390/bdcc9080210

Smmarwar, S. K., Gupta, G. P., & Kumar, S. (2024). Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review. *Telematics and Informatics Reports, 14*, 100130. https://doi.org/10.1016/j.teler.2024.100130

Sullivan, G. M., & Artino, A. R., Jr. (2013). Analyzing and interpreting data from Likert-type scales. *Journal of Graduate Medical Education, 5*(4), 541-542. https://doi.org/10.4300/JGME-5-4-18

Taherdoost, H. (2016). Validity and reliability of the research instrument: How to test the validation of a questionnaire/survey in a research. *International Journal of Academic Research in Management, 5*(3), 28-36. https://doi.org/10.2139/ssrn.3205040

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications, 238*, 122199. https://doi.org/10.1016/j.eswa.2023.122199