ANALISIS TINGKAT KESADARAN KEAMANAN SIBER TERHADAP TINDAKAN PREVENTIF SISWA SMKN 1 BANDAR LAMPUNG JURUSAN TEKNIK JARINGAN KOMPUTER DAN TELEKOMUNIKASI

(Skripsi)

Oleh

MUHAMMAD IRGHI FAHREZI
NPM 2213025055

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2026

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER TERHADAP TINDAKAN PREVENTIF SISWA SMKN 1 BANDAR LAMPUNG JURUSAN TEKNIK JARINGAN KOMPUTER DAN TELEKOMUNIKASI

Oleh

MUHAMMAD IRGHI FAHREZI

Skripsi

Sebagai Salah Satu Syarat Untuk Mencapai Gelar

SARJANA PENDIDIKAN

Pada
Program Studi Pendidikan Teknologi Informasi
Jurusan Pendidikan Ilmu Pengetahuan Alam
Fakultas Keguruan Dan Ilmu Pendidikan
Universitas Lampung

FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2026

ABSTRAK

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER TERHADAP TINDAKAN PREVENTIF SISWA SMKN 1 BANDAR LAMPUNG JURUSAN TEKNIK JARINGAN KOMPUTER DAN TELEKOMUNIKASI

Oleh

MUHAMMAD IRGHI FAHREZI

Penelitian ini bertujuan untuk mengetahui hubungan tingkat kesadaran keamanan siber terhadap tindakan preventif siswa SMKN 1 Bandar Lampung jurusan Teknik Jaringan Komputer dan Telekomunikasi. Penelitian ini menggunakan jenis deskriptif dengan pendekatan kuantitatif. Populasi penelitian adalah seluruh siswa jurusan Teknik Jaringan Komputer dan Telekomunikasi SMKN 1 Bandar Lampung, dengan sampel yang ditentukan melalui teknik *proportional random sampling*.

Responden dalam penelitian ini berjumlah 176 siswa, yang terdiri dari 130 siswa laki-laki (73,9%) dan 46 siswa perempuan (26,1%). Data diperoleh melalui penyebaran kuesioner yang telah diuji validitas dan reabilitasnya, didukung dengan observasi dan dokumentasi. Data dianalisis menggunakan statistik deskriptif, korelasi.

Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber siswa berada pada kategori cukup hingga tinggi, sedangkan tindakan preventif siswa tergolong cukup baik namun belum sepenuhnya konsisten. Berdasarkan analisis inferensial, diperoleh bahwa terdapat hubungan positif dan signifikan antara kesadaran keamanan siber dengan tindakan preventif siswa, dengan nilai koefisien korelasi sebesar r = 0,996 dan nilai signifikansi sebesar 0,000 < 0,05, yang berarti semakin tinggi tingkat kesadaran keamanan siber maka semakin baik pula tindakan preventif yang dilakukan siswa. Implikasi dari penelitian ini menunjukkan bahwa sekolah perlu memperkuat program literasi keamanan siber melalui pembelajaran, pelatihan, dan praktik langsung agar kesadaran siswa tidak hanya bersifat pengetahuan, tetapi juga terwujud dalam perilaku nyata yang konsisten dalam menjaga keamanan digital.

Kata kunci: Kesadaran Keamanan Siber, Siswa SMK, Keamanan Digital, Tindakan Preventif.

ABSTRACT

ANALYSIS OF THE LEVEL OF CYBERSECURITY AWARENESS ON PREVENTIVE ACTIONS OF STUDENTS AT SMKN 1 BANDAR LAMPUNG COMPUTER NETWORK AND TELECOMMUNICATIONS ENGINEERING DEPARTMENT

By

MUHAMMAD IRGHI FAHREZI

This study aims to examine the relationship between the level of cybersecurity awareness and the preventive actions of students at SMKN 1 Bandar Lampung, majoring in Computer and Network Engineering and Telecommunications. This research employs a descriptive method with a quantitative approach. The population of this study consists of all students in the Computer and Network Engineering and Telecommunications major at SMKN 1 Bandar Lampung, with the sample determined using proportional random sampling. The respondents in this study were 176 students, consisting of 130 male students (73.9%) and 46 female students (26.1%). Data were collected through questionnaires that had been tested for validity and reliability, supported by observation and documentation. Data analysis was conducted using descriptive statistics and correlation analysis. The results of the study indicate that students' level of cybersecurity awareness falls within the moderate to high category, while their preventive actions are considered fairly good but not yet fully consistent. Based on inferential analysis, it was found that there is a positive and significant relationship between cybersecurity awareness and students' preventive actions, with a correlation coefficient of $r = 0.996$ and a significance value of $0.000 < 0.05$. This implies that the higher the level of cybersecurity awareness, the better the preventive actions performed by students. The implications of this study suggest that schools need to strengthen cybersecurity literacy programs through learning activities, training, and practical implementation so that students' awareness is not only theoretical but also reflected in consistent real-life digital security practices.

Keywords: Cybersecurity Awareness, Preventive Actions, Vocational School Students, Digital Security.

Judul Skripsi	:	**ANALISIS TINGKAT KESADARAN KEAMANAN SIBER TERHADAP TINDAKAN PREVENTIF SISWA SMKN 1 BANDAR LAMPUNG JURUSAN TEKNIK JARINGAN KOMPUTER DAN TELEKOMUNIKASI**
Nama Mahasiswa	:	***Muhammad Irghi Fahrezi***
Nomor Pokok Mahasiswa	:	**2213025055**
Program Studi	:	**Pendidikan Teknologi Informasi**
Jurusan	:	**Pendidikan MIPA**
Fakultas	:	**Keguruan dan Ilmu Pendidikan**

MENYETUJUI

1. **Komisi Pembimbing**

Pembimbing Utama	Pembimbing Pembantu
Dr Afif Rahman Riyanda, S.Pd., M.Pd.	**Daniel Rinaldi, S.T., M.Eng.**
NIK 231804900716101	NIP 199305052022031008

2. Ketua Jurusan Pendidikan MIPA

Dr. Nurhanurawati, M.Pd.
NIP. 196708081991032001

MENGESAHKAN

1. Tim Penguji

Ketua : **Dr. Afif Rahman Riyanda, M.Pd.T.** .....

Sekretaris : **Daniel Rinaldi, S.T., M.Eng.** .....

Penguji
Bukan Pembimbing : **Dr. Rangga Firdaus, S.Kom., M.Kom.** .....

2. Dekan Fakultas Keguruan dan Ilmu Pendidikan

Dr. Albet Maydiantoro, M.Pd.
NIP 19870504 201404 1 001

Tanggal Lulus Ujian Skripsi : 16 April 2026

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS LAMPUNG
JURUSAN PENDIDIKAN ILMU PENGETAHUAN SOSIAL
Jl. Prof. Dr. Sumantri Brojonegoro No.1 Gedong Meneng - Bandar Lampung 35145
Telepon (0721) 704624, Faximile (0721) 704624
e-mail: fkip@unila.ac.id, laman: http://fkip.unila.ac.id

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Muhammad Irghi Fahrezi
NPM	: 2213025055
Program Studi	: Pendidikan Teknologi Informasi
Jurusan	: Pendidikan MIPA
Fakultas	: Keguruan dan Ilmu Pendidikan

Dengan ini saya menyatakan bahwa skripsi yang berjudul "Analisis Tingkat Kesadaran Keamanan Siber Terhadap Tindakan Preventif Siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi" adalah benar hasil karya saya sendiri dan bukan karya orang lain. Seluruh tulisan yang termuat dalam skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti bahwa skripsi ini adalah hasil jiplakan atau telah dibuat oleh orang lain sebelumnya, maka saya bersedia menerima sanksi sesuai dengan ketentuan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya.

Bandar Lampung, 10 April 2026

Muhammad Irghi Fahrezi
2213025055

RIWAYAT HIDUP

Penulis dilahirkan pada tanggal 28 Desember 2003 di Pardasuka Kabupaten Pringsewu, sebagai anak kedua dari dua bersaudara, dari Ibu Bernama Juhainah dan Ayah Bernama M. Hasbi Nawawi. Penulis menyelesaikan pendidikan formal pertama kali di Sekolah Dasar (SD) Negeri 1 Poncowati Lampung Tengah tahun 2016, Menyelesaikan Sekolah Menengah Pertama (SMP) di SMP Negeri 1 Terbanggi Besar Lampung Tengah tahun 2019, kemudian melanjutkan jenjang Sekolah Menengah Kejuruan (SMK) di SMK Negeri 2 Terbanggi Besar Kabupaten Lampung Tengah dan lulus tahun 2022.

Pada Tahun 2022, penulis terdaftar sebagai mahasiswa di Program Studi Pendidikan Teknologi Informasi Fakultas Keguruan dan Ilmu Pendidikan Universitas Lampung melalui jalur SBMPTN. Penulis melakukan Kuliah Kerja Nyata (KKN) di Desa Sumberejo Kecamatan Tumijajar Kabupaten Tulang Bawang Barat dan Praktik Lapangan Persekolahan (PLP) di SMPN 25 Tulang Bawang Barat. Kemudian di pertengahan tahun 2025, penulis melakukan Praktik Industri (PI) di BANK SYARIAH INDONESIA. Selama menjadi mahasiswa, penulis aktif dalam organisasi internal kampus bersama Dewan Perwakilan Mahasiswa Fakultas (DPM-F) dengan menjabat sebagai Ketua Komisi II Dewan Perwakilan Mahasiswa Fakultas tahun 2024-2025, Badan Eksekutif Mahasiswa Fakultas (BEM-F) sebagai Sekretaris Umum pada tahun 2025-2026, serta mejadi bagian dari Forum Pendidikan Teknologi Informasi (FORMATIF) sebagai anggota Divisi Mikat pada tahun 2022-2023.

MOTTO

“Jika sempit hidup ini
Tidur selalu tak tenang
Pagi selalu menyiksa
Semua akan baik saja
Sebab Tuhan tlah berjanji
Setelah sempit ada kemudahan.”

(Raim Laode, Bersenja Gurau)

"Siapapun yang memulai perjalanan dengan bersinar, ia pun akan berakhir dengan bersinar."

(Syeikh Ibnu Athaillah)

"Aku tidak peduli siapa yang lebih hebat dariku, aku harus jauh lebih hebat dari diriku di tahun lalu, ini adalah aku vs aku."

(Penulis)

PERSEMBAHAN

Puja dan puji syukur saya panjatkan kepada Allah SWT atas segala kenikmatan-Nya

Sehingga skripsi ini dapat diselesaikan tepat waktu.

Yang paling kusayangi dan kubanggakan, skripsi ini kupersembahkan untuk kedua orang tuaku dari hasil jerih payah yang kujalani selama 4 tahun ini.

Terimakasih untuk seluruh cinta dan kasihmu untuk anakmu.

Terimakasih telah mengasihi, melindungi, dan menjaga diriku dengan penuh kesabaran serta tetes keringat air mata.

Keluarga Pendidikan Teknologi Informasi 2022.

Serta Almamater Tercinta,

Universitas Lampung.

SANWACANA

Puji syukur penulis ucapkan kepada Allah SWT, atas segala berkat, rahmat dan karunia-Nya, penulis dapat menyelesaikan penyusunan skripsi ini. Penulisan skripsi yang berjudul "Analisis Tingkat Kesadaran Keamanan Siber Terhadap Tindakan Preventif Siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi". Yang merupakan salah satu syarat untuk memperoleh gelar sarjana Pendidikan pada Fakultas Keguruan dan Ilmu Pendidikan Universitas Lampung.

Penulis menyadari sepenuhnya dalam penulisan skripsi ini tidak terlepas dari motivasi, doa, bimbingan, dan bantuan masukan dari berbagai pihak. Untuk itu, dalam kesempatan ini penulis menyampaikan terima kasih secara tulus kepada:

1. Ibu Prof. Dr. Ir. Lusmeilia Afriani, D.E.A., IPM., ASEAN., Eng. Selaku Rektor Universitas Lampung.
2. Bapak Dr. Albet Maydiantoro, S.Pd., M.Pd., selaku Dekan FKIP Universitas Lampung.
3. Bapak Dr. Riswandi, M.Pd., selaku Wakil Dekan Bidang Akademik dan Kerjasama FKIP Universitas Lampung.
4. Bapak Bambang Riadi, S.Pd., M.Pd., selaku wakil Dekan Bidang Umum dan Keuangan
5. Bapak Hermi Yanzi, S.Pd., M.Pd., selaku Wakil Dekan Bidang Kemahasiswaan dan Alumni FKIP Universitas Lampung.
6. Ibu Dr. Nurhanurawati, M.Pd., selaku Ketua Jurusan Pendidikan MIPA
7. Ibu Dr. Pramudiyanti, S.Si., M.Si., sebagai Ketua Program Studi Pendidikan Teknologi Informasi.
8. Bapak Dr. Afif Rahman Riyanda, S.Pd., M.Pd.T., selaku dosen pembimbing 1. Terimakasih telah meluangkan waktu, pikiran serta tenaga untuk memberikan bimbingan, arahan, motivasi serta perhatian dengan penuh kesabaran selama penulis melakukan proses penyusunan skripsi ini. Semoga

segala kebaikan dan ilmu yang telah diberikan mendapatkan balasan yang berlipat ganda oleh Allah SWT.

9. Bapak Daniel Rinaldi, S.T., M.Eng., selaku dosen pembimbing 2 dan Pembimbing Akademik. Terima kasih telah meluangkan waktu dan memberikan kritikan, arahan, saran masukannya kepada penulis yang berguna dalam penyempurnaan skripsi ini. Semoga segala kebaikan dan ilmu yang telah diberikan mendapatkan balasan yang berlipat ganda oleh Tuhan YME.
10. Bapak Dr. Rangga Firdaus, S.Kom., M.Kom., selaku dosen pembahas saya. Terima kasih bapak yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan saran, kritik, serta solusi dalam proses pembahasan skripsi ini. Semoga segala kebaikan dan ilmu yang telah diberikan mendapatkan balasan yang berlipat ganda oleh Allah Swt.
11. Untuk Ayah dan Ibu, terima kasih atas doa yang tidak pernah putus, sabar yang tidak pernah habis, dan dukungan yang selalu menguatkan di saat aku lelah dan hampir menyerah. Setiap langkah dalam perjuanganku, selalu ada kalian di belakangku, memberi kekuatan tanpa banyak kata. Apa pun yang kucapai hari ini dan nanti, semua tidak lepas dari cinta, pengorbanan, dan keikhlasan kalian. Terima kasih sudah menjadi alasan terbesarku untuk terus bertahan dan berjuang.
12. Untuk cinta pertamaku, Ibu Juhainah. perjalanan kuliah ini bukan hanya tentang aku, tapi tentang dirimu yang diam-diam ikut lelah bersamaku. Saat aku mengeluh, kau menahan letihmu sendiri. Saat aku hampir menyerah, kau tetap berdiri, meski kakimu juga gemetar. Doa-doamu mungkin tak terdengar, tapi aku tahu Tuhan selalu mendengarnya lebih dulu dariku. Jika suatu hari namaku dipanggil karena keberhasilan, ketahuilah, di balik itu ada air mata, sabar, dan cintamu yang tidak pernah meminta balasan. Aku berjalan dengan kakiku, tapi aku sampai karena hatimu yang tidak pernah lelah mengantarku Terima kasih, cinta pertamaku, atas cinta yang terlalu besar untuk sekadar kubalas dengan kata.
13. Untuk Abangku, Muhammad Adam Fahreza, terima kasih sudah menjadi sosok yang selalu menguatkan, meski sering tanpa banyak kata. Di saat aku ragu, kehadiranmu memberi rasa aman, di saat aku lelah, caramu mendukung membuatku tetap melangkah. Mungkin tidak selalu terlihat, tapi peranmu

selalu ada dalam setiap perjuanganku. Terima kasih, Bang, sudah menjadi pelindung, penyemangat, dan contoh tentang arti tanggung jawab dalam keluarga.

15. Untuk kamu yang selalu ada di sisiku, Aradia Rosalino. terima kasih karena memilih bertahan di saat aku tidak selalu mudah untuk dipahami. Di balik lelah dan sibukku, kamu tetap hadir dengan sabar, dukungan, dan doa yang tidak pernah putus. Kamu bukan hanya teman berbagi tawa, tapi juga tempat pulang saat aku hampir menyerah. Terima kasih sudah berjalan bersamaku, tanpa banyak tuntutan, hanya dengan cinta yang tulus.
16. Bapak dan Ibu Dosen Program Studi Pendidikan Teknologi Informasi yang telah memberikan ilmu dan pengalaman hidup selama penulis menjadi mahasiswa.
17. Teruntuk teman-teman Terbaikku, yaitu Aldi Surya Purnama, Akhmad Danu Damara, Fatih Muhammad Sulung Z, Nyoman Arda Herawan, dan M. Ikmal Khoiru Zad. Terima kasih atas kebersamaan, dukungan, serta tawa yang telah mewarnai setiap perjalanan selama masa perkuliahan hingga sampai di fase skripsi ini. Terima kasih telah hadir di sela-sela padatnya tugas, namun selalu mampu kalian ubah menjadi momen penuh semangat dan kebahagiaan. Setiap saran, kritik, dan bantuan yang kalian berikan telah menjadi bagian penting dalam proses belajar dan tumbuh bersama. Semoga semangat dan kebersamaan ini terus terjaga hingga nanti, ketika masing-masing dari kita menapaki jalan menuju impian dan karier yang diharapkan. Semangat untuk kita semua, Semoga setelah menyelesaikan studi ini, kita semua dapat diterima di tempat kerja yang kita impikan, menjadi pribadi yang sukses dan tetap rendah hati, serta tidak melupakan kisah indah yang telah kita ukir bersama.
18. Teruntuk teman-teman seperjuangan serta Kanda dan Yunda di HMI Komisariat KIP Universitas Lampung, terima kasih atas setiap proses yang kita lalui bersama. Dari diskusi, perdebatan, hingga tawa sederhana, semua menjadi bagian yang membentuk kedewasaan dan jati diri saya. Di HMI, saya belajar arti bertahan, memahami, dan menghargai dalam setiap dinamika. HMI bukan sekadar organisasi, tetapi rumah untuk tumbuh sebagai mahasiswa dan manusia. Semoga kebersamaan ini tidak hanya menjadi kenangan, melainkan terus hidup sebagai nilai dalam setiap langkah kita ke depan.

19. Terima kasih kepada teman-teman yang telah menemani perjalanan saya sejak bangku sekolah hingga perkuliahan. Kebersamaan, dukungan, dan kenangan yang kita lalui bersama menjadi bagian berharga dalam hidup saya. Semoga persahabatan ini tetap terjaga dan kita semua meraih kesuksesan di masa depan.
20. Teman-teman mahasiswa Pendidikan Teknologi Informasi angkatan 2022 terima kasih atas dukungan dan kerja sama selama menempuh pendidikan hingga dapat menyelesaikan studi, dapat menggapai cita-cita dan mimpi, serta dapat membanggakan kedua orang tua.
21. Teruntuk teman-teman Pendidikan Teknologi Informasi kelas A yang telah menjadi bagian penting dalam perjalanan perkuliahan ini. Terima kasih atas setiap kebersamaan, semangat, dan dukungan yang telah diberikan sejak awal memasuki dunia perkuliahan hingga pada tahap akhir penyusunan skripsi ini.
22. Teruntuk teman-teman KKN dan PLP Desa Sumber Rejo, pengalaman ini menjadi momen berharga yang tidak terlupakan. Terima kasih kepada Bapak Sulis beserta keluarga, khususnya atas kebaikan dan sambutan hangat selama kami berada di posko. Kebersamaan tidak hanya terjalin dalam pelaksanaan program kerja, tetapi juga melalui momen sederhana seperti memancing dan bermain bersama yang mempererat kekompakan.
23. Teruntuk seluruh Guru di SMKN 1 Bandar Lampung, Terimakasih telah memberikan dukungan, bimbingan, serta bantuan selama proses penelitian ini berlangsung. Tanpa arahan, kerja sama, dan kesediaan waktu yang diberikan, penelitian ini tidak akan dapat terselesaikan dengan baik. Semoga segala kebaikan dan bantuan yang telah diberikan mendapatkan balasan yang setimpal.
24. Siswa/i yang sudah berkontribusi untuk menjadi bagian dari responden. Terima kasih atas bantuan dan kerjasamanya dalam memberikan respon kuesioner yang baik. Semoga Allah SWT selalu mempermudah segala urusan kalian dan hal-hal baik selalu menyertai kalian.
25. Kakak tingkat 2021, 2020 dan 2019 yang tidak dapat disebutkan satu per satu terima kasih atas arahan, motivasi dan bantuannya, semoga Allah SWT mempermudah segala urusan kalian.
26. Semua pihak yang telah membantu dan mendoakan dalam penyelesaian skripsi ini baik secara langsung dan tidak langsung, semoga Allah SWT selalu memberikan kemurahan dan melimpah atas kebaikan dan balasan yang

berlipat ganda bagi kita semua.

27. Terima kasih kepada Almamater Tercinta Universitas Lampung yang sudah memberikan banyak ilmu dan membuat saya banyak berkembang. Semoga ilmu yang saya dapatkan dapat saya gunakan untuk memajukan bangsa dan negara serta membawa nama harum Unila.

Disadari sepenuhya bahwa dalam penulisan skripsi ini masih jauh dari sempurna, oleh karna itu saran dan kritik yang bersifat membangun selalu diharapkan oleh penulis, semoga skripsi ini bermanfaat bagi penulis khususnya dan bagi pembaca pada umumnya

Bandar Lampung, 10 April 2026

Penulis

Muhammad Irghi Fahrezi

DAFTAR ISI

Halaman

DAFTAR ISI ..... **i**
DAFTAR TABEL ..... **iv**
DAFTAR GAMBAR ..... **vi**
DAFTAR LAMPIRAN ..... **vii**

BAB I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Rumusan Masalah 5
1.3. Tujuan Penelitian 5
1.4. Manfaat Penelitian 6

BAB II TINJAUAN PUSTAKA **7**
2.1. Kajian Teori 8
2.2. Kajian Literatur 8
2.2.1. Kesadaran Keamanan Siber 8
2.2.2. Tindakan Preventif 10
2.2.3. Hubungan Kesadaran dengan Tindakan Preventif 15
2.3. Penelitian Terdahulu 18
2.4. Pendekatan Teoritis yang Digunakan 19
2.5. Kerangka Pikir 19

BAB III METODE PENELITIAN **21**
3.1. Jenis dan Pendekatan Penelitian 21
3.2. Populasi dan Sampel 22
3.3. Variabel Penelitian 23
3.4. Definisi Operasional Variabel 24
3.5. Instrumen Penelitian 25
3.6. Teknik Pengumpulan Data 33
3.7. Teknik Analisis Data 34
3.7. Statistik Inferensial 36
3.8. Hipotesis Statistik 38

BAB IV HASIL DAN PEMBAHASAN 39
4.1. Deskripsi Lokasi Penelitian 39
4.1.1 Sejarah Singkat SMKN 1 Bandar Lampung 39
4.1.2 Visi dan Misi SMKN 1 Bandar Lampung 40
4.2. Gambaran Umum Responden 40
4.3. Teknik Analisis Data 41
4.3.1 Analisis Statistik Deskriptif 41
4.3.2 Analisis Statistik Hasil Indikator 42
4.4 Analisis Statistik Inferensial 46
..4.4.1 Uji Prasyarat Analisis 47
4.5. Pengujian Hipotesis Statistik 49
4.6. Pembahasan Hasil Penelitian 55
4.7. Implikasi Temuan Penelitian 77

BAB V SIMPULAN DAN SARAN 79
5.1. Simpulan 79
5.2. Saran 80

DAFTAR PUSTAKA 81

LAMPIRAN 89

DAFTAR TABEL

Tabel Halaman

1. Penelitian Terdahulu 18
2. Data Jumlah Siswa Jurusan TJKT 22
3. Definisi Operasional 25
4. Uji Validitas Instrumen Kesadaran Keamanan Siber 27
5. Kesimpulan Hasil Uji Validitas Instrumen Tingkat Kesadaran Keamanan Siber (X) 29
6. Uji Validitas Instrumen Tindakan Preventif 29
7. Kesimpulan Hasil Uji Validitas Instrumen Tindakan Preventif (Y) 31
8. Interpretasi Koefisien r 32
9. Uji Hasil Uji Reliabilitas 32
10. Kategori Interpretasi Persentase 36
11. Statistik Deskriptif Variabel Penelitian 41
12. Hasil Rekapitulasi Jawaban Responden Per indikator Variabel X dan Y. 43
13. Hasil Rekapitulasi Jawaban Responden Berdasarkan Indikator Variabel X dan Y yang Dikelompokkan Menurut Gender 44
14. Hasil Uji Normalitas Data 47
15. Hasil Uji Linearitas Variabel X dan Variabel Y 48
16. Hasil Uji Homogenitas 48
17. Uji Hipotesis Berdasarkan Gender 49
18. Uji Hipotesis Berdasarkan Kelas 50
19. Uji Hipotesis Berdasarkan Gender dan Kelas 51
20. Hasil Uji Hipotesis X terhadap Y 54

DAFTAR GAMBAR

Gambar Halaman

1. Kerangka Pikir 19
2. Diagram Batang Statistik Deskriptif Variabel X dan Y 42
3. Diagram Perbandingan Rata-rata Berdasarkan Angkatan 52
4. Grafik Korelasi X Terhadap Y 55

DAFTAR LAMPIRAN

Lampiran Halaman

1. Surat Izin Pra-Penelitian 90
2. Surat Balasan Izin Pra-Penelitian 91
3. Surat Izin Penelitian 92
4. Surat Balasan Izin Penelitian 93
5. Kisi-Kisi Angket Penelitian 94
6. Angket Penelitian 99
7. Penyebaran Kuesioner Penelitian Pada Siswa Kelas X, XI, XII Jurusan TJKT 102
8. Uji Validitas Instrumen 103
9. Uji Reabilitas Instrumen 110
10. Tabulasi Data 111
11. Uji Normalitas 117
12. Uji Linearitas 118
13. Uji Homogenitas 119
14. Uji Hipotesis X terhadap Y 120
15. Uji Hipotesis Variabel X Terhadap Y Berdasarkan Gender 121
16. Uji Hipotesis Berdasarkan Kelas 121
17. Uji Hipotesis Berdasarkan Gender dan Kelas 123

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang sangat pesat membawa dampak positif dalam berbagai aspek kehidupan, termasuk dunia pendidikan. Di satu sisi, kemajuan ini memungkinkan terjadinya transformasi digital melalui pemanfaatan Teknologi Informasi dan Komunikasi (TIK), seperti internet cepat, aplikasi pembelajaran berbasis cloud, serta platform digital yang memungkinkan guru dan siswa berinteraksi tanpa batas ruang dan waktu. Hal ini sejalan dengan pendapat Balaban, Rienties, dan Winne (2023) yang menyatakan bahwa integrasi TIK dalam pendidikan mampu meningkatkan kualitas pembelajaran, memperluas akses sumber belajar, serta mendorong terciptanya inovasi dalam proses mengajar dan belajar.

Namun, di sisi lain, perkembangan teknologi informasi juga menghadirkan ancaman serius berupa kejahatan siber yang menyasar semua kalangan, termasuk pelajar. Oleh karena itu, kesadaran keamanan siber (*cybersecurity awareness*) menjadi aspek penting yang perlu ditanamkan sejak dini agar generasi muda mampu melindungi data dan informasi pribadinya dari potensi serangan siber. Siswa Sekolah Menengah Kejuruan (SMK), khususnya jurusan Teknik Jaringan Komputer dan Telekomunikasi (TJKT), memiliki peran strategis dalam dunia digital. Siswa dipersiapkan menjadi tenaga terampil yang akan terjun langsung dalam bidang teknologi informasi (Yildiz Durak, 2022). Dengan demikian, kemampuan siswa dalam memahami dan menerapkan tindakan preventif keamanan siber sangat penting untuk mendukung kesiapan menghadapi ancaman dunia kerja digital yang semakin kompleks.

Keamanan siber dapat dipahami sebagai seperangkat aktivitas, kebijakan, proses, dan kontrol yang dirancang untuk melindungi sistem informasi, jaringan, perangkat keras dan lunak, serta data dari ancaman digital yang mencakup akses tidak sah, pencurian, perusakan, maupun gangguan operasional. Schiliro (2023) menegaskan bahwa keamanan siber merupakan gabungan sumber daya, infrastruktur, serta proses yang berfungsi melindungi sistem digital dari kejadian yang mengompromikan integritas dan hak milik. Sejalan dengan itu, penelitian oleh Dospinescu *et al*. (2024) menekankan bahwa keamanan siber tidak hanya sebatas aspek teknis, tetapi juga mencakup pendidikan dan pembelajaran interaktif untuk meningkatkan kesadaran generasi muda terhadap ancaman dan metode perlindungan digital. Di Indonesia, Kristianti dan Kurniasi (2023) menekankan pentingnya regulasi dan kebijakan hukum sebagai pilar dalam menjaga keamanan siber di tengah pesatnya perkembangan teknologi digital. Dengan demikian, keamanan siber dapat dipandang secara komprehensif sebagai upaya perlindungan yang bersifat teknis, edukatif, maupun regulatif dalam menghadapi tantangan dunia maya yang semakin kompleks.

Secara teoritis, kesadaran keamanan siber dapat dipahami sebagai tingkat pemahaman individu mengenai ancaman digital, perilaku yang aman, serta kepatuhan terhadap aturan keamanan teknologi informasi. Teori perilaku terencana (*Theory of Planned Behavior*) menjelaskan bahwa kesadaran seseorang akan memengaruhi niat dan tindakannya (Abawajy & Kim, 2020). Dengan demikian, siswa yang memiliki tingkat kesadaran keamanan siber yang baik cenderung lebih mampu melakukan tindakan preventif dalam aktivitas digitalnya. Secara empiris, penelitian menunjukkan bahwa rendahnya kesadaran siber dapat meningkatkan kerentanan individu terhadap serangan seperti *phishing, malware*, dan pencurian identitas. Misalnya, penelitian di kalangan siswa sekolah menengah menunjukkan bahwa kurangnya pengetahuan dan keterampilan dasar keamanan siber membuat mereka lebih rentan terhadap ancaman digital (Setyaningrum *et al*., 2023).

Serangan siber membawa berbagai dampak serius bagi individu, organisasi, maupun negara. Beberapa penelitian menunjukkan bahwa serangan dapat menyebabkan kerusakan data, gangguan layanan publik, hingga melumpuhkan sistem vital seperti administrasi imigrasi dan pusat data nasional yang berakibat pada kerugian ekonomi serta menurunnya kepercayaan masyarakat terhadap pemerintah (Soekarno-Hatta Airport Case, 2024). Selain itu, kasus ransomware di Kementerian Kominfo juga memperlihatkan risiko kebocoran data sensitif akibat lemahnya pengelolaan infrastruktur digital dan minimnya backup, yang pada akhirnya merusak reputasi institusi (Telkom University Journal, 2024). Dampak tersebut juga berimbas pada stabilitas ekonomi karena organisasi harus menanggung biaya pemulihan, denda regulasi, hingga kehilangan pelanggan (ScienceDirect, 2024).

Untuk mengatasi permasalahan ini, sejumlah solusi ditawarkan, antara lain memperkuat regulasi keamanan siber agar sejalan dengan standar internasional, meningkatkan kemampuan sumber daya manusia melalui pendidikan dan pelatihan, serta mengadopsi teknologi canggih seperti enkripsi, autentikasi multi-faktor, dan sistem deteksi berbasis kecerdasan buatan. Selain itu, diperlukan kolaborasi lintas sektor serta pengembangan infrastruktur digital yang aman melalui mekanisme backup, pembaruan perangkat lunak, dan perbaikan sistem lama yang rentan (Indus Publishers, 2024; arXiv, 2025).

Salah satu aspek penting yang perlu diperhatikan adalah hubungan antara tingkat pengetahuan, sikap, dan praktik keamanan siber. Penelitian terbaru menemukan bahwa meskipun sebagian siswa mengetahui ancaman siber, namun tindakan preventif nyata seperti penggunaan kata sandi yang kuat atau verifikasi dua langkah masih jarang dilakukan (Öz & Yildirim, 2022). Konteks pendidikan vokasi di Indonesia, termasuk SMKN 1 Bandar Lampung, menuntut adanya penelitian yang lebih spesifik. Siswa jurusan TJKT tidak hanya menggunakan internet untuk belajar, tetapi juga terlibat dalam praktik jaringan dan administrasi sistem yang rawan diserang jika tidak memahami protokol keamanan. Oleh sebab

itu, kajian tentang tingkat kesadaran keamanan siber dan hubungannya dengan tindakan preventif sangat relevan dilakukan.

Beberapa penelitian terdahulu memberikan gambaran berharga untuk penelitian ini. Studi di Turki menemukan bahwa siswa SMA memiliki tingkat kesadaran siber yang rendah, terutama dalam aspek teknis seperti pengelolaan kata sandi (Öz & Yildirim, 2022). Temuan ini menjadi sangat relevan dalam konteks siswa SMK Jurusan Teknik Jaringan Komputer dan Telekomunikasi (TJKT) di Indonesia, yang secara khusus dipersiapkan sebagai tenaga ahli bidang teknologi. Misalnya, penelitian di SMK Telkom Purwokerto menunjukkan bahwa dengan pemberian pelatihan praktis seperti teknik *footprinting* dan *reconnaissance*, siswa TKJ dapat meningkatkan pemahaman siswa tentang ancaman siber serta kemampuan dalam mengidentifikasi titik lemah pada sistem keamanan (Prabowo *et al*., 2024). Selain itu, kegiatan sosialisasi keamanan siber di SMK N 2 Salatiga juga menemukan bahwa setelah pelatihan, siswa menjadi lebih berhati-hati dalam penggunaan media sosial dan menunjukkan peningkatan keterampilan dalam mengamankan akun digital pribadi mereka (Candra Wulan *et al*., 2022). Kedua studi ini memperkuat asumsi bahwa meskipun siswa SMK TJKT memiliki basis teknis sebagai keunggulan, kesadaran siber siswa tidak otomatis tinggi dan tetap memerlukan intervensi melalui pelatihan maupun sosialisasi untuk meningkatkan aspek teknis sekaligus perilaku keamanan digital.

Penelitian lain menunjukkan bahwa pembelajaran berbasis kesadaran siber dapat meningkatkan keterampilan preventif siswa. Misalnya, penerapan program pelatihan keamanan siber terbukti meningkatkan kesadaran dan kemampuan siswa dalam menghindari serangan *phishing* (Torten & Yael, 2021). Hal ini memperkuat justifikasi empiris bahwa intervensi pendidikan dapat mengubah perilaku siswa. Namun demikian, masih terbatas penelitian di Indonesia, khususnya pada tingkat SMK jurusan TJKT, yang menyoroti hubungan antara kesadaran dan tindakan preventif. Hal ini membuka peluang penelitian baru yang tidak hanya mendeskripsikan kondisi, tetapi juga menguji hubungan kausal antarvariabel. Dengan begitu, penelitian ini dapat memberikan kontribusi akademis dan praktis.

Berdasarkan uraian di atas, penelitian berjudul **"Analisis Tingkat Kesadaran Keamanan Siber terhadap Tindakan Preventif Siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi"** menjadi penting dan layak dilakukan. Hasil penelitian diharapkan dapat memberikan rekomendasi strategis bagi sekolah dalam merancang kurikulum atau pelatihan tambahan mengenai keamanan siber, sehingga siswa tidak hanya memiliki pengetahuan teknis, tetapi juga keterampilan preventif yang memadai.

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana perbedaan tingkat kesadaran keamanan siber dan Tindakan preventif siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi berdasarkan gender dan angkatan/tingkatan kelas?
2. Bagaimana tingkat kesadaran keamanan siber siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi?
3. Apakah terdapat hubungan yang signifikan antara tingkat kesadaran keamanan siber dengan tindakan preventif siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi?

1.3. Tujuan Penelitian

Tujuan penelitian masalah dalam penelitian ini adalah:

1. Untuk mengetahui perbedaan tingkat kesadaran keamanan siber dan tindakan preventif siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi berdasarkan gender dan angkatan/tingkatan kelas.
2. Untuk mengetahui bagaimana tingkat kesadaran keamanan siber siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi

3. Untuk mengetahui apakah terdapat hubungan yang signifikan antara tingkat kesadaran keamanan siber dengan tindakan preventif siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi

1.4. Manfaat Penelitian

1. Manfaat Teoritis / Akademis

Penelitian ini diharapkan dapat menambah khazanah ilmu pengetahuan dalam bidang keamanan siber pendidikan, khususnya terkait kesadaran siswa terhadap ancaman digital. Memberikan gambaran empiris mengenai hubungan antara tingkat kesadaran keamanan siber dengan tindakan preventif siswa, sehingga dapat memperkuat teori tentang perilaku keamanan digital di kalangan remaja. Menjadi rujukan akademis untuk penelitian sejenis di masa depan, terutama dalam pengembangan model pembelajaran atau intervensi yang berfokus pada *cyber security awareness* di lingkungan sekolah kejuruan.

2. Manfaat Praktis

a) Bagi Sekolah

Memberikan rekomendasi strategi untuk meningkatkan kesadaran keamanan siber siswa, misalnya melalui kurikulum tambahan, pelatihan, atau simulasi keamanan digital.

b) Bagi Siswa

Membantu mereka memahami pentingnya tindakan preventif dalam menghadapi ancaman siber sehingga lebih bijak dalam menggunakan internet, media sosial, maupun perangkat jaringan.

c) Bagi pihak terkait

Menjadi dasar pertimbangan dalam merumuskan kebijakan atau program peningkatan literasi keamanan digital di sekolah menengah kejuruan.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Kesadaran keamanan siber (*cybersecurity awareness*) merupakan elemen penting dalam melindungi individu maupun organisasi dari ancaman digital. Menurut Albar dan Musadieq (2024), kesadaran keamanan siber tidak hanya berkaitan dengan pemahaman teknis, tetapi juga perilaku pengguna dalam menerapkan praktik aman di dunia maya, seperti penggunaan kata sandi yang kuat, kewaspadaan terhadap *phishing*, dan kepatuhan pada kebijakan keamanan yang berlaku.

Di lingkungan pendidikan, terutama sekolah menengah kejuruan dengan jurusan yang berhubungan langsung dengan teknologi, kesadaran keamanan siber menjadi semakin krusial. Penelitian Hakim (2022) menunjukkan bahwa siswa yang memiliki pemahaman tentang risiko siber lebih cenderung melakukan tindakan preventif, misalnya mengaktifkan autentikasi ganda dan memperbarui perangkat lunak secara berkala. Dengan demikian, kesadaran dapat dipandang sebagai faktor prediktif terhadap perilaku pencegahan.

Lebih jauh, Albar dan Musadieq (2024) menegaskan bahwa literasi digital dan pelatihan keamanan berpengaruh signifikan terhadap tingkat kesadaran. Hal ini sejalan dengan pandangan Pratiwi dan Setyaningrum (2023) yang menyoroti pentingnya integrasi kurikulum keamanan siber dalam dunia pendidikan, karena keterpaparan siswa terhadap materi keamanan akan meningkatkan perilaku aman dalam aktivitas daring sehari-hari.

Kesadaran keamanan siber merupakan faktor kunci dalam melindungi individu maupun organisasi dari ancaman digital, yang tidak hanya mencakup aspek teknis tetapi juga perilaku aman pengguna. Di lingkungan pendidikan, khususnya sekolah menengah kejuruan yang berkaitan dengan teknologi, kesadaran ini berperan penting karena siswa dengan pemahaman risiko siber terbukti lebih cenderung melakukan tindakan preventif. Berbagai penelitian juga menegaskan bahwa literasi digital, pelatihan, serta integrasi kurikulum keamanan siber memiliki pengaruh signifikan dalam meningkatkan kesadaran dan membentuk perilaku aman siswa dalam aktivitas daring sehari-hari.

2.2 Kajian Literatur

2.2.1 Kesadaran Keamanan Siber

Kesadaran keamanan siber (*cybersecurity awareness*) merupakan pemahaman, sikap, dan perilaku individu dalam menggunakan teknologi informasi secara aman untuk mengurangi risiko serangan siber. Dalam konteks pendidikan, khususnya di sekolah kejuruan yang berfokus pada bidang teknologi, kesadaran ini menjadi penting karena siswa sering terlibat langsung dalam praktik jaringan komputer dan penggunaan perangkat berbasis internet.

Menurut penelitian (Mubarak *et al*., 2021), kesadaran keamanan siber dipengaruhi oleh pengetahuan, sikap, dan praktik yang dilakukan oleh individu. Ketiganya saling berhubungan; pengetahuan yang baik akan membentuk sikap positif, yang kemudian mendorong praktik aman dalam aktivitas digital.

2.2.1.1 Pengetahuan (Knowledge)

Pengetahuan merupakan komponen utama dari kesadaran keamanan siber. Menurut Hidayat *et al*. (2023), pengetahuan tentang ancaman siber secara signifikan memengaruhi sikap dan perilaku preventif siswa,

termasuk dalam hal pengelolaan kata sandi, kewaspadaan terhadap *phishing*, dan penggunaan perangkat lunak asli.

Selain itu, Putri *et al*. (2024) menemukan bahwa siswa SMK dengan tingkat pengetahuan tinggi cenderung lebih aktif dalam menerapkan langkah-langkah pencegahan seperti backup data dan penggunaan autentikasi ganda. Namun, penelitian Nugroho *et al*. (2020) menunjukkan masih banyak siswa dan mahasiswa yang belum memiliki pemahaman memadai tentang ancaman siber, terutama terkait *social engineering* dan keamanan media sosial.

2.2.1.2 Sikap (*Attitude*)

Sikap terhadap keamanan siber mencakup keyakinan, persepsi, serta kecenderungan respon siswa dalam menghadapi ancaman digital. Studi menunjukkan bahwa sikap positif terhadap keamanan siber berhubungan erat dengan peningkatan kepatuhan pada aturan dan kebijakan keamanan. Misalnya, penelitian di Indonesia menemukan bahwa sikap siswa terhadap keamanan siber berpengaruh signifikan terhadap tingkat kesadaran dan kepatuhan terhadap praktik keamanan digital (Suhartini *et al.*, 2022).

Selain itu, sikap siswa dipengaruhi oleh faktor pengalaman menggunakan teknologi, pendidikan tentang keamanan siber, serta persepsi terhadap risiko. Semakin tinggi pemahaman tentang potensi kerugian akibat serangan siber, semakin positif pula sikap siswa dalam mengantisipasi ancaman (Nugroho *et al*., 2022).

2.2.1.3 Perilaku (*Behavior*)

Perilaku mengacu pada tindakan nyata siswa dalam menjaga keamanan siber, seperti penggunaan kata sandi yang kuat, tidak membagikan informasi pribadi, dan menghindari akses ke situs berbahaya. Penelitian terbaru di kalangan siswa SMK di Indonesia

menemukan bahwa perilaku pencegahan sangat dipengaruhi oleh sikap serta pemahaman mereka tentang keamanan siber. Siswa yang memiliki sikap positif lebih cenderung menerapkan tindakan preventif seperti memperbarui perangkat lunak, menggunakan autentikasi ganda, dan meningkatkan kewaspadaan terhadap *phishing* (Wijayanto & Susanto, 2023).

Lebih lanjut, faktor lingkungan sekolah dan dukungan guru juga turut berperan dalam membentuk perilaku siswa terhadap keamanan siber. Edukasi yang diberikan secara konsisten mampu memperkuat kebiasaan positif siswa, sehingga tindakan preventif terhadap ancaman siber dapat menjadi rutinitas sehari-hari (Putra *et al*., 2021).

2.2.2 Tindakan Preventif

Tindakan preventif keamanan siber adalah serangkaian langkah pencegahan yang dilakukan individu maupun organisasi untuk melindungi sistem, data, dan jaringan dari potensi ancaman siber. Tujuan utama dari tindakan ini adalah meminimalisasi risiko serangan, mencegah kebocoran data, serta menjaga keberlangsungan layanan digital. Menurut ENISA (*European Union Agency for Cybersecurity*, 2021), tindakan preventif tidak hanya mencakup aspek teknis, tetapi juga kebijakan organisasi dan perilaku individu dalam penggunaan teknologi. Hal ini berarti kesadaran, keterampilan, dan disiplin pengguna menjadi faktor penting dalam menciptakan lingkungan digital yang aman.

Selain itu, Wulandari *et al*. (2021) menekankan bahwa tindakan preventif dapat diwujudkan melalui praktik sederhana namun signifikan, seperti penggunaan kata sandi yang kuat, pembaruan perangkat lunak secara berkala, dan kewaspadaan dalam berbagi informasi pribadi. Langkah-langkah ini dapat mengurangi kerentanan terhadap serangan umum seperti *phishing, malware*, maupun *ransomware*. Dengan kata lain, tindakan preventif bukan hanya tanggung jawab teknis semata, tetapi juga

mencerminkan budaya keamanan digital yang harus dibangun secara kolektif baik di lingkungan pendidikan, organisasi, maupun masyarakat luas.

2.2.2.1 Penggunaan Kata Sandi yang Kuat dan Autentikasi Ganda

Penggunaan kata sandi yang kuat merupakan salah satu langkah paling dasar namun vital dalam menjaga keamanan akun digital. Kata sandi yang efektif biasanya terdiri dari kombinasi huruf besar, huruf kecil, angka, dan simbol, serta tidak menggunakan informasi pribadi yang mudah ditebak seperti tanggal lahir, nama, atau pola sederhana. Selain itu, pengguna disarankan untuk mengganti kata sandi secara berkala agar meminimalisasi risiko penyalahgunaan. Menurut penelitian Alotaibi (2022), lemahnya pengelolaan kata sandi menjadi salah satu faktor utama meningkatnya kasus pencurian akun, sehingga literasi digital terkait manajemen kata sandi harus diperkuat sejak dini.

Autentikasi ganda (*Two-Factor Authentication/2FA*) melengkapi keamanan kata sandi dengan menambahkan lapisan verifikasi tambahan, misalnya melalui kode OTP (*One Time Password*) yang dikirimkan ke ponsel, email, atau aplikasi autentikasi khusus. Dengan mekanisme ini, meskipun kata sandi berhasil diretas, akun tetap terlindungi karena peretas memerlukan akses tambahan yang sulit diperoleh. ENISA (2021) menegaskan bahwa 2FA merupakan salah satu praktik terbaik yang sangat efektif dalam mencegah akses tidak sah. Sejalan dengan itu, Wulandari *et al*. (2021) juga menekankan bahwa kombinasi antara kata sandi yang kuat dan autentikasi ganda dapat secara signifikan mengurangi kerentanan pengguna terhadap serangan *phishing* maupun *brute force*. Dengan demikian, kesadaran akan pentingnya penerapan dua aspek ini menjadi fondasi utama dalam membangun keamanan digital yang berkelanjutan.

2.2.2.2 Pembaruan Perangkat Lunak dan Sistem Operasi

Pembaruan perangkat lunak dan sistem operasi merupakan salah satu indikator penting dalam tindakan preventif keamanan siber. Setiap pembaruan umumnya dirancang untuk memperbaiki bug, meningkatkan performa, dan terutama menutup celah kerentanan (*security vulnerabilities*) yang dapat dimanfaatkan oleh peretas. Jika pengguna mengabaikan pembaruan ini, maka perangkat mereka menjadi lebih rentan terhadap serangan *malware, ransomware*, maupun eksploitasi sistem oleh pihak tidak bertanggung jawab. Oleh karena itu, pembaruan secara rutin menjadi langkah krusial dalam menjaga integritas serta keamanan data digital (Wulandari *et al*., 2021).

Selain itu, studi oleh Nunes *et al*. (2022) menegaskan bahwa sebagian besar serangan siber modern menargetkan perangkat dengan *software* yang sudah usang atau tidak diperbarui. Praktik seperti menunda *update* atau menonaktifkan notifikasi pembaruan meningkatkan peluang terjadinya kompromi data. Untuk itu, pengguna disarankan mengaktifkan fitur *auto-update* atau secara proaktif melakukan pembaruan manual. Dengan langkah ini, sistem dapat lebih terlindungi dari ancaman baru yang terus berkembang di ekosistem digital (ENISA, 2021; Nunes *et al*., 2022).

2.2.2.3 Kewaspadaan dalam Berbagi Informasi Pribadi

Kewaspadaan dalam berbagi informasi pribadi merupakan indikator penting dalam upaya preventif keamanan siber karena data sensitif dapat dimanfaatkan untuk berbagai bentuk kejahatan digital. Informasi sederhana seperti alamat email, nomor telepon, atau tanggal lahir sering kali menjadi pintu masuk bagi pelaku kejahatan untuk melakukan *phishing,* rekayasa sosial, atau bahkan pencurian identitas. Menurut ENISA (2021), sebagian besar serangan berbasis rekayasa sosial berhasil karena individu kurang menyadari nilai dari data pribadi yang mereka bagikan secara sembarangan di *platform* digital. Oleh karena itu, kehati-

hatian dalam mengunggah informasi di media sosial maupun mengisi data pada situs yang tidak terpercaya sangat diperlukan untuk meminimalisasi risiko.

Kesadaran ini menjadi semakin penting bagi siswa SMK jurusan Teknik Jaringan Komputer dan Telekomunikasi (TJKT) yang aktif menggunakan internet dan media digital dalam kegiatan belajar maupun komunikasi sehari-hari. Penelitian oleh Alqaralleh & Alqatawna (2021) menunjukkan bahwa generasi muda sering kali menjadi target utama kejahatan berbasis identitas karena aktivitas daring mereka yang tinggi serta kecenderungan berbagi informasi secara terbuka. Dengan memahami risiko penyebaran data pribadi, siswa dapat mengurangi potensi pencurian identitas, penyalahgunaan akun, hingga serangan manipulasi psikologis yang semakin marak di era digital.

2.2.2.4 *Backup* Data Secara Berkala

Backup data secara berkala merupakan strategi antisipatif yang sangat penting untuk mencegah kerugian akibat serangan siber, seperti *ransomware*, yang dapat mengunci akses terhadap data pengguna dan meminta tebusan agar akses dikembalikan. Dengan melakukan backup pada perangkat eksternal atau layanan *cloud* yang aman, pengguna dapat memulihkan data penting meskipun sistem utama terserang, mengalami kerusakan, atau kehilangan akses. Menurut Wulandari *et al*. (2021), praktik backup tidak hanya mengurangi risiko kehilangan data, tetapi juga mempercepat proses pemulihan sistem.

Selain itu, *backup* juga berfungsi menjaga keberlangsungan aktivitas akademik maupun profesional. Bagi siswa SMK TJKT, kebiasaan melakukan backup sangat relevan karena mereka kerap bekerja dengan data proyek jaringan, konfigurasi server, hingga hasil praktik laboratorium yang bersifat krusial. Kehilangan data tanpa *backup* dapat berdampak signifikan terhadap kelanjutan pembelajaran dan evaluasi

kompetensi teknis. Penelitian oleh Xia *et al*. (2020) menegaskan bahwa *backup reguler*, terutama melalui sistem otomatis berbasis *cloud,* menjadi langkah fundamental dalam strategi manajemen risiko siber modern karena mampu memberikan redundansi dan keandalan data yang tinggi. Dengan demikian, *backup* bukan hanya tindakan preventif, tetapi juga bagian integral dari budaya keamanan digital yang perlu ditanamkan sejak dini.

2.2.2.5 Pemanfaatan Jaringan dan Perangkat yang Aman

Pemanfaatan jaringan dan perangkat yang aman merupakan salah satu indikator kunci dalam tindakan preventif keamanan siber. Mengakses internet melalui jaringan *Wi-Fi* publik tanpa perlindungan sangat berisiko karena data dapat dengan mudah disadap oleh pihak yang tidak bertanggung jawab. Untuk itu, penggunaan *Virtual Private Network (VPN)* serta penerapan enkripsi data sangat dianjurkan guna menjaga kerahasiaan dan integritas informasi yang dikirim maupun diterima. ENISA (2021) menegaskan bahwa kesadaran akan risiko jaringan publik yang tidak aman harus ditanamkan sejak dini agar pengguna mampu mengambil langkah pencegahan yang tepat.

Selain perlindungan jaringan, keamanan perangkat juga menjadi faktor yang tidak kalah penting. Perangkat digital, baik komputer maupun ponsel, perlu dilengkapi dengan antivirus terkini, *firewall* aktif, serta pengaturan keamanan sesuai standar agar terlindungi dari serangan *malware, spyware*, maupun pencurian data. Penelitian oleh Alotaibi (2019) menunjukkan bahwa perilaku pengguna yang tidak mengaktifkan fitur keamanan perangkat meningkatkan risiko paparan serangan siber hingga 60%. Bagi siswa SMK TJKT, pemahaman tentang pentingnya penggunaan perangkat dan jaringan yang aman sangat relevan karena mereka dipersiapkan untuk menghadapi dunia kerja digital yang sarat tantangan. Dengan demikian, penerapan kebiasaan menggunakan jaringan serta perangkat yang aman bukan hanya melindungi data

pribadi, tetapi juga membentuk fondasi profesionalisme dalam bidang teknologi informasi.

2.2.3 Hubungan Kesadaran dengan Tindakan Preventif

Kesadaran merupakan faktor penting yang memengaruhi perilaku seseorang dalam melakukan tindakan preventif, termasuk dalam konteks keamanan siber. Semakin tinggi tingkat kesadaran seseorang terhadap risiko yang ada, semakin besar kemungkinan ia untuk mengambil langkah pencegahan yang tepat. Dalam dunia pendidikan, khususnya pada siswa SMK yang bergelut dengan teknologi jaringan komputer dan telekomunikasi, kesadaran terhadap ancaman siber akan mendorong perilaku yang lebih hati-hati dan tindakan pencegahan yang lebih baik.

Penelitian menunjukkan bahwa terdapat hubungan positif antara tingkat kesadaran keamanan siber dengan perilaku pencegahan yang dilakukan pengguna. Siswa atau individu yang memiliki kesadaran lebih tinggi cenderung lebih disiplin dalam melaksanakan praktik keamanan digital, seperti penggunaan kata sandi yang kuat, kewaspadaan terhadap *phishing,* dan pemeliharaan perangkat lunak keamanan (Ardiyanto *et al*., 2022).

2.2.3.1 Pengetahuan Teknis

Kesadaran keamanan siber merupakan salah satu faktor penting yang memengaruhi tindakan preventif dalam melindungi data dan sistem. Pada konteks siswa Sekolah Menengah Kejuruan (SMK), khususnya jurusan Teknik Jaringan Komputer dan Telekomunikasi, pengetahuan teknis menjadi landasan utama dalam mengembangkan kesadaran yang berorientasi pada praktik pencegahan. Menurut penelitian (Kurniawan *et al.*, 2023), siswa dengan tingkat pemahaman teknis yang baik cenderung lebih sadar terhadap ancaman siber dan mampu menerapkan langkah-langkah pencegahan, seperti penggunaan kata sandi yang kuat, autentikasi ganda, dan pembaruan sistem. Hal ini menunjukkan bahwa

pengetahuan teknis berperan langsung dalam membentuk perilaku preventif.

Lebih lanjut, penelitian (Tanjung *et al*., 2024) menekankan bahwa kesadaran keamanan siber di kalangan siswa vokasi meningkat signifikan ketika diberikan pelatihan teknis dasar, seperti konfigurasi jaringan aman dan deteksi ancaman *phishing*. Artinya, penguasaan teknis tidak hanya meningkatkan keterampilan, tetapi juga memperkuat kesadaran dalam bertindak preventif.

2.2.3.2 Sikap terhadap Resiko

Sikap terhadap risiko mencerminkan cara individu merespons ancaman keamanan digital. Penelitian menunjukkan bahwa siswa dengan tingkat kesadaran yang baik memiliki kecenderungan lebih tinggi untuk bersikap waspada dan mengambil langkah pencegahan, seperti mengatur kata sandi dengan baik, tidak sembarangan mengklik tautan, dan menjaga kerahasiaan data pribadi.

Menurut Sulistiani & Puspitarini (2021), kesadaran keamanan berbanding lurus dengan sikap terhadap risiko, di mana mahasiswa yang memahami potensi ancaman lebih berhati-hati dalam aktivitas digitalnya. Hal serupa ditegaskan oleh Susanti *et al*. (2021) bahwa kesadaran keamanan siber mendorong perilaku mitigasi risiko saat pembelajaran daring.

2.2.3.3 Kebiasaan Digital

Kebiasaan digital merupakan manifestasi nyata dari kesadaran keamanan siber dalam kehidupan sehari-hari. Individu dengan kebiasaan digital yang baik cenderung lebih sering menerapkan praktik aman, misalnya rutin memperbarui perangkat, menggunakan autentikasi ganda, serta membatasi akses informasi pribadi. Purba (2022) menemukan bahwa literasi digital yang baik, termasuk pemahaman keamanan,

membentuk kebiasaan digital yang lebih aman di kalangan pelajar. Sementara itu, Rohman & Putra (2021) menekankan bahwa kebiasaan digital siswa yang dipengaruhi kesadaran keamanan, seperti penggunaan *password* yang kuat dan etika bermedia sosial, memiliki korelasi kuat dengan perilaku pencegahan serangan siber.

2.2.3.4 Lingkungan Belajar

Lingkungan belajar memiliki peran penting dalam membentuk kesadaran siswa mengenai keamanan siber. Kesadaran yang baik dapat mendorong siswa untuk mengambil tindakan preventif dalam menghadapi ancaman digital. Menurut beberapa penelitian, lingkungan pendidikan yang mendukung, baik melalui kurikulum maupun praktik pembelajaran, dapat meningkatkan pemahaman dan sikap siswa terhadap keamanan informasi. Penelitian oleh (Putri *et al*., 2021) menunjukkan bahwa model pembelajaran yang interaktif, seperti penggunaan peta konsep, mampu meningkatkan kesadaran siswa dalam memahami materi kompleks, termasuk topik terkait literasi digital. Hal ini menandakan bahwa lingkungan belajar yang mendorong keterlibatan aktif dapat memperkuat kesadaran.

Selain itu, (Utami *et al*., 2023) menemukan bahwa pendekatan edutainment dalam pembelajaran sains berkontribusi dalam meningkatkan kesadaran siswa terhadap isu-isu praktis dalam kehidupan, termasuk keamanan teknologi. Dengan demikian, metode pembelajaran yang menyenangkan dapat memengaruhi sikap siswa dalam mengambil langkah preventif. Dalam konteks keamanan siber, (Anisa *et al*., 2023) menekankan pentingnya literasi digital dan etika digital di sekolah menengah kejuruan. Hasil penelitiannya mengindikasikan bahwa siswa dengan tingkat kesadaran digital yang tinggi lebih cenderung menerapkan tindakan preventif, seperti penggunaan kata sandi yang kuat dan kewaspadaan terhadap penipuan *online.*

2.3 Penelitian Yang Relevan

Penelitian yang relevan adalah hasil penelitian terdahulu yang relevan dan dapat dijadikan sebagai titik tolak penelitian yang akan dilakukan. Peneliti memilih penelitian yang berkaitan dan memiliki relevansi dengan penelitian yang akan dilakukan. Berbagai macam penelitian terdahulu ini digunakan sebagai acuan dan bahan pertimbangan dalam melaksanakan penelitian. Penelitian relevan yang akan digunakan sebagai acuan dalam pembuatan penelitian ini.

Tabel 1. Penelitian Yang Relevan

Nama Peneliti	Tahun	Judul	Metode	Temuan
Anshori	2023	Literasi Keamanan Siber dalam Dunia Pendidikan	Studi literatur	Literasi keamanan siber di kalangan pelajar masih rendah, siswa perlu dibekali pemahaman dasar tentang perlindungan data pribadi dan etika digital (Anshori, 2023).
Huda	2022	*Cyber Security Awareness* pada Siswa SMK di Era Digital	Survei kuantitatif	Mayoritas siswa memiliki kesadaran rendah terkait *phishing, password management,* dan keamanan jaringan sekolah (Huda, 2022).
Ariyanto & Sari	2021	Analisis Tingkat Kesadaran Keamanan Informasi pada Mahasiswa	Kuantitatif deskriptif	Mahasiswa cenderung memahami aspek teknis, namun abai pada tindakan preventif seperti *update* perangkat lunak dan penggunaan autentikasi ganda (Ariyanto & Sari, 2021).
Putra	2020	Kesadaran Privasi Digital Generasi Z di Indonesia	*Mixed method*	Generasi Z memiliki kebiasaan berbagi informasi berlebihan di media sosial, menunjukkan kesenjangan antara pengetahuan dan perilaku keamanan digital (Putra, 2020).

Dari penelitian-penelitian pada tabel 1, dapat disimpulkan bahwa kesadaran keamanan siber di kalangan siswa/mahasiswa Indonesia masih relatif rendah, terutama dalam tindakan preventif seperti manajemen kata sandi, pencegahan *phishing*, dan menjaga privasi digital. Hal ini memperkuat urgensi penelitian

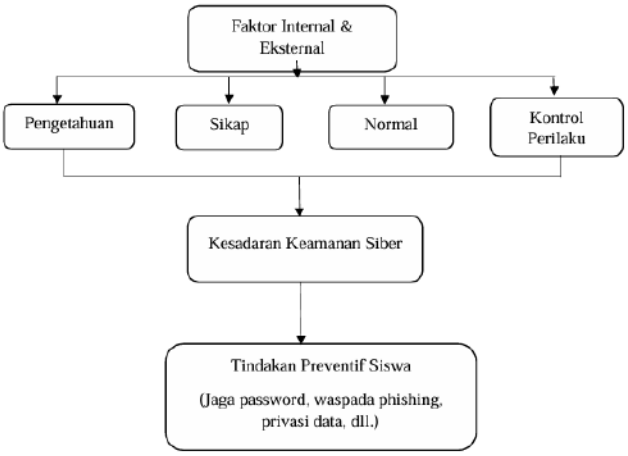
yang dilakukan pada siswa SMKN 1 Bandar Lampung jurusan Teknik Jaringan Komputer dan Telekomunikasi.

2.4 Pendekatan Teoritis yang Digunakan

Penelitian mengenai kesadaran keamanan siber pada siswa maupun masyarakat umumnya menggunakan pendekatan teoritis dari *Cybersecurity Awareness Model, Theory of Planned Behavior* (*TPB*), serta *Technology Acceptance Model* (*TAM*). Pendekatan ini membantu menjelaskan faktor psikologis, perilaku, dan teknologi yang memengaruhi tindakan preventif terhadap ancaman siber.

2.5 Kerangka Pikir

Kerangka berpikir pada gambar menunjukkan bahwa tindakan preventif siswa dalam keamanan siber dipengaruhi oleh kesadaran keamanan siber. Kesadaran tersebut terbentuk dari faktor internal dan eksternal yang mencakup pengetahuan, sikap, norma, dan kontrol perilaku. Semakin baik keempat faktor tersebut, maka semakin tinggi kesadaran keamanan siber siswa. Kesadaran yang tinggi kemudian mendorong siswa untuk melakukan tindakan preventif, seperti menjaga kata sandi, waspada terhadap phishing, dan melindungi privasi data.



Gambar 1. Kerangka Berfikir

Kerangka Pikir penelitian ini dapat dirumuskan sebagai berikut:

1. Kesadaran keamanan siber siswa dipengaruhi oleh faktor pengetahuan, sikap, norma sosial, dan kontrol perilaku.
2. Tingkat kesadaran ini berimplikasi pada tindakan preventif yang dilakukan siswa, seperti menjaga kerahasiaan akun, menghindari tautan mencurigakan, dan menggunakan perangkat dengan aman.
3. Semakin tinggi kesadaran siswa, semakin besar kemungkinan mereka untuk menerapkan perilaku aman dalam menghadapi ancaman siber.

Berdasarkan uraian tersebut, kerangka pikir penelitian ini divisualisasikan pada Gambar 1 yang menggambarkan alur hubungan antara faktor-faktor pembentuk kesadaran keamanan siber dengan tindakan preventif siswa. Dengan demikian, penelitian ini didasarkan pada asumsi bahwa kesadaran keamanan siber berpengaruh langsung terhadap tindakan preventif siswa. Oleh karena itu, pengukuran tingkat kesadaran keamanan siber dapat digunakan untuk memprediksi sejauh mana siswa menerapkan praktik keamanan digital yang baik.

BAB III
METODE PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan kuantitatif. Pendekatan kuantitatif dipilih karena penelitian ini berfokus pada pengukuran numerik tingkat kesadaran keamanan siber siswa serta analisis hubungannya dengan tindakan preventif yang mereka lakukan. Data yang diperoleh akan diolah menggunakan teknik statistik sehingga dapat menggambarkan pola, tren, dan hubungan antarvariabel secara objektif (Cahya *et al*., 2023).

Jenis penelitian deskriptif dipilih karena tujuan utama penelitian ini adalah untuk menggambarkan kondisi nyata kesadaran keamanan siber siswa jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung. Penelitian deskriptif kuantitatif dapat memberikan informasi rinci mengenai tingkat pengetahuan, sikap, serta perilaku preventif siswa terhadap ancaman siber (Pratama & Arief, 2022).

Pendekatan kuantitatif juga memungkinkan peneliti untuk melakukan generalisasi terhadap populasi penelitian melalui analisis data yang bersifat numerik. Dengan demikian, hasil penelitian diharapkan dapat menjadi dasar rekomendasi strategis bagi sekolah dalam meningkatkan literasi dan kesadaran keamanan siber siswa (Kurniawan & Putra, 2021).

3.2 Populasi dan Sampel

3.2.1. Populasi

Populasi dalam penelitian ini adalah seluruh siswa SMKN 1 Bandar Lampung yang tergabung dalam Jurusan Teknik Jaringan Komputer dan

Telekomunikasi (TJKT). Populasi dipilih karena siswa jurusan ini memiliki keterkaitan langsung dengan bidang teknologi informasi dan komunikasi sehingga tingkat kesadaran terhadap keamanan siber menjadi isu penting yang relevan untuk diteliti. Dengan demikian, populasi penelitian ini mencakup seluruh siswa aktif jurusan TJKT pada tahun ajaran 2025/2026, yang jumlahnya disajikan pada tabel 2.

Tabel 2. Data Jumlah Siswa Jurusan TJKT

No	Angkatan	Jumlah
1	Kelas X	108
2	Kelas XI	106
3	Kelas XII	101
	Jumlah	**315**

Sumber: Absensi Siswa Jurusan TJKT 2025/2026.

3.2.2 Sampel

Sampel penelitian adalah sebagian dari populasi yang dianggap dapat mewakili keseluruhan karakteristik populasi (Sugiyono, 2019). Teknik pengambilan sampel yang digunakan adalah *proportional random sampling*, yaitu pengambilan sampel secara acak dengan mempertimbangkan proporsi jumlah siswa di setiap tingkat kelas (X, XI, XII) pada jurusan TJKT.

Jumlah sampel ditentukan dengan menggunakan rumus *Slovin*, karena populasi diketahui secara pasti dan penelitian ini bersifat kuantitatif dengan keterbatasan waktu serta sumber daya (Sevilla *et al*., 1960; Umar, 2013). Rumus *Slovin* adalah:

$$n = \frac{N}{1 + N\ (e^2)}$$

Keterangan:

n = jumlah sampel

N = jumlah populasi

e = tingkat kesalahan (*margin of error*), dalam penelitian ini ditetapkan sebesar 5% (0,05)

Berdasarkan rumus diatas besarnya sampel dalam penelitian adalah:

$$n = \frac{315}{1 + 315\ (0{,}05)^2}$$

n = 176,2 dibulatkan menjadi 176

Jadi menurut perhitungan diatas, besarnya sampel dalam penelitian ini adalah sebanyak 176 responden.

Dengan menerapkan rumus tersebut, jumlah sampel yang diperoleh akan didistribusikan secara proporsional pada masing-masing tingkat kelas sehingga representasi siswa tetap terjaga. Pemilihan responden dalam tiap kelas dilakukan secara acak sederhana (*simple random*), sehingga setiap siswa memiliki peluang yang sama untuk menjadi sampel penelitian.

3.3. Variabel Penelitian

Variabel penelitian merupakan segala sesuatu yang menjadi fokus pengamatan dalam suatu penelitian, yang berfungsi untuk menjawab pertanyaan penelitian serta menguji hipotesis yang telah dirumuskan. Dalam penelitian ini, variabel dibagi menjadi dua, yaitu variabel bebas (independen) dan variabel terikat (dependen).

3.3.1 Variabel Bebas (*Independent Variable*)

Variabel bebas adalah variabel yang memengaruhi atau menjadi sebab terjadinya perubahan pada variabel lain. Dalam penelitian ini, variabel bebas adalah tingkat kesadaran keamanan siber siswa. Kesadaran keamanan siber mencakup pemahaman, pengetahuan, serta sikap siswa mengenai praktik keamanan dalam penggunaan perangkat teknologi informasi dan komunikasi. Indikator variabel bebas ini dapat meliputi:

1. Pengetahuan tentang ancaman siber (misalnya *phishing, malware,* pencurian data).
2. Pemahaman mengenai penggunaan *password* yang kuat dan aman.
3. Kesadaran dalam menjaga kerahasiaan informasi pribadi.

4. Sikap terhadap penggunaan perangkat lunak legal dan aman.
5. Tindakan waspada saat mengakses internet, media sosial, maupun email

3.3.2 Variabel Terikat (*Dependent Variable*)

Variabel terikat adalah variabel yang dipengaruhi oleh variabel bebas, atau yang menjadi akibat dari adanya perlakuan terhadap variabel bebas. Dalam penelitian ini, variabel terikat adalah tindakan preventif siswa terhadap ancaman siber. Tindakan preventif dimaksudkan sebagai langkah nyata yang dilakukan siswa untuk mencegah terjadinya ancaman atau serangan siber. Indikator variabel terikat ini dapat meliputi:

1. Kebiasaan memperbarui perangkat lunak dan aplikasi secara berkala.
2. Menggunakan autentikasi ganda atau metode keamanan tambahan.
3. Menjaga kerahasiaan data pribadi saat menggunakan internet.
4. Menghindari akses terhadap situs atau aplikasi yang berisiko.
5. Membuat cadangan data penting secara rutin.

3.4 Definisi Operasional Variabel

Definisi Operasional Variabel untuk mempermudah pengukuran dan analisis dalam penelitian ini, diperlukan penjabaran mengenai definisi operasional dari setiap variabel yang diteliti. Definisi operasional variabel digunakan untuk menjelaskan makna konseptual dan batasan empiris dari masing-masing variabel agar dapat diukur secara kuantitatif. Dengan demikian, setiap variabel memiliki indikator yang jelas dan dapat diobservasi sesuai dengan tujuan penelitian. Adapun definisi operasional variabel dalam penelitian ini pada table 3.

Tabel 3. Definisi Operasional

Variabel	Uraian Konsep	Indikator	Skala
Kesadaran Keamanan Siber	Tingkat pengetahuan, pemahaman, dan sikap siswa mengenai ancaman serta praktik keamanan digital. Kesadaran ini mencakup pengetahuan teknis, sikap terhadap risiko, dan kebiasaan menjaga keamanan data (Aini *et al*., 2023).	1. Pengetahuan (*Knowledge*) b. Sikap (*Attitude*) c. Perilaku (*Behavior*) (Fitriah *et al*., 2022)	Skala Likert (1–5) melalui kuesioner: sangat tidak sadar sangat sadar.
Tindakan Preventif Keamanan Siber	Upaya nyata siswa untuk melindungi perangkat dan data pribadi dari ancaman siber, misalnya dengan penggunaan teknologi atau kebiasaan aman (Setyawan & Suryanto, 2021).	a. Penggunaan Kata Sandi yang Kuat dan Autentikasi Ganda b. Pembaruan Perangkat Lunak dan Sistem Operasi c. Kewaspadaan dalam Berbagi Informasi Pribadi d. Backup Data Secara Berkala e. Pemanfaatan Jaringan dan Perangkat yang Aman (Wulandari *et al*. 2021)	Skala Likert (1–5) melalui kuesioner: sangat jarang sangat sering.

3.5. Instrumen Penelitian

3.5.1 Jenis Penelitian

Instrumen penelitian yang digunakan adalah kuesioner (angket) dengan skala Likert. Kuesioner ini dipilih karena mampu mengukur sikap, persepsi, dan tingkat kesadaran siswa secara kuantitatif terhadap keamanan siber. Responden akan diminta memberikan tingkat persetujuan terhadap pernyataan yang berkaitan dengan kesadaran keamanan siber, mulai dari "sangat tidak setuju" hingga "sangat setuju". Metode ini dinilai efektif karena dapat menjaring data dalam jumlah besar secara cepat serta

memberikan gambaran yang terukur mengenai tindakan preventif siswa terhadap ancaman siber (Ardhian *et al*., 2020).

Setiap indikator penelitian, seperti kesadaran penggunaan kata sandi, privasi data, serta perilaku aman saat menggunakan internet, akan dituangkan dalam item pertanyaan dengan skala 1–5. Skala Likert dipandang sesuai karena mampu menangkap variasi tingkat persetujuan responden secara bertahap dan telah banyak digunakan dalam penelitian terkait literasi digital dan keamanan informasi (Handayani & Prasetyo, 2020); (Rachmawati et al., 2021).

3.5.2 Uji Validitas instrument

Validitas instrumen menunjukkan sejauh mana suatu instrumen mampu mengukur variabel yang dimaksud secara tepat dan akurat (Sugiyono, 2019). Suatu instrumen dinyatakan valid apabila dapat mengungkapkan data yang sesuai dan relevan dengan variabel yang sedang diteliti, sehingga hasil pengukuran dapat dipercaya untuk menggambarkan kondisi sebenarnya. Dalam penelitian ini, validitas diuji menggunakan teknik korelasi *Product Moment Pearson*. Teknik ini digunakan untuk mengetahui seberapa besar hubungan antara skor masing-masing item pernyataan dengan skor total keseluruhan (Azwar, 2017). Jika hasil korelasi menunjukkan nilai signifikan dan positif, maka item tersebut dinyatakan valid. Rumus yang digunakan adalah sebagai berikut:

$$r_{xy} = \frac{N \Sigma XY - (\Sigma X)(\Sigma Y)}{\sqrt{\{N \Sigma X^2 - (\Sigma X)^2\}} \sqrt{\{N \Sigma Y^2 - (\Sigma Y)^2\}}}$$

Keterangan:

R_{xy} = Koefisien korelasi antara variable X dan Y

N = Jumlah peserta tes (testee)

$\sum xy$ = Total perkiraan skor item dansoal

$\sum x$ = Jumlah skor butir pernyataan

$\sum y$ = Jumlah Skortotal

$\sum x^2$ = Jumlah kuadrat skor butirpernyataan

$\sum y^2$ = Jumlah kuadrat skor total

Berdasarkan dengan Kriteria pengujian jika harga $r_{hitung} > r_{tabel}$ dengan alpha = 0,5 dan n sampel yang diteilti, maka alat ukur tersebut valid, begitu pula sebaliknya jika harga rhitung ≤ r_{tabel} maka alat ukur tersebut tidak valid (Rusman, 2024: 37).

3.5.2.1 Hasil Uji Validitas Instrumen

Uji validitas dilakukan untuk mengetahui sejauh mana butir pernyataan dalam kuesioner mampu mengukur variabel yang diteliti. Pengujian validitas dilakukan dengan membandingkan nilai r hitung dengan r tabel pada taraf signifikansi 0,05 dengan jumlah responden 176 (r tabel = 0,294). Butir pernyataan dinyatakan valid apabila nilai r hitung lebih besar dari r tabel.

3.5.2.1.1 Uji Validitas Variabel X (Tingkat Kesadaran Keamanan Siber)

Instrumen variabel tingkat kesadaran keamanan siber terdiri dari 20 butir pernyataan. Berdasarkan hasil pengujian, diperoleh bahwa 16 butir pernyataan dinyatakan valid karena memiliki nilai r_{hitung} lebih besar dari r_{tabel}. Sementara itu, 4 butir pernyataan dinyatakan tidak valid karena nilai r_{hitung} lebih kecil dari r_{tabel}. Butir pernyataan yang valid selanjutnya digunakan dalam analisis penelitian.

Tabel 4. Uji Validitas Instrumen Tingkat Kesadaran Keamanan Siber

No	Item	r Hitung	r Tabel (0,294)	Kondisi	Simpulan
1	Butir 1	0,612	0,294	r hitung > r tabel	Valid
2	Butir 2	0,584	0,294	r hitung > r tabel	Valid
3	Butir 3	0,498	0,294	r hitung > r tabel	Valid
4	Butir 4	0,721	0,294	r hitung > r tabel	Valid
5	Butir 5	0,463	0,294	r hitung > r tabel	Valid
6	Butir 6	0,689	0,294	r hitung > r tabel	Valid

No	Item	r Hitung	r Tabel (0,294)	Kondisi	Simpulan
7	Butir 7	0,542	0,294	r hitung > r tabel	Valid
8	Butir 8	0,311	0,294	r hitung > r tabel	Valid
9	Butir 9	0,157	0,294	r hitung < r tabel	Tidak Valid
10	Butir 10	0,604	0,294	r hitung > r tabel	Valid
11	Butir 11	0,579	0,294	r hitung > r tabel	Valid
12	Butir 12	0,142	0,294	r hitung < r tabel	Tidak Valid
13	Butir 13	0,687	0,294	r hitung > r tabel	Valid
14	Butir 14	0,521	0,294	r hitung > r tabel	Valid
15	Butir 15	0,498	0,294	r hitung > r tabel	Valid
16	Butir 16	0,133	0,294	r hitung < r tabel	Tidak Valid
17	Butir 17	0,566	0,294	r hitung > r tabel	Valid
18	Butir 18	0,612	0,294	r hitung > r tabel	Valid
19	Butir 19	0,149	0,294	r hitung < r tabel	Tidak Valid
20	Butir 20	0,634	0,294	r hitung > r tabel	Valid

Sumber: Data hasil pengolahan menggunakan SPSS, 2025

Berdasarkan hasil uji validitas instrumen variabel Tingkat Kesadaran Keamanan Siber pada tabel 4, pengujian dilakukan terhadap 20 butir pernyataan dengan jumlah responden sebanyak 45 siswa. Uji validitas dilakukan dengan membandingkan nilai r hitung masing-masing butir pernyataan dengan nilai r_{tabel} sebesar 0,294 pada taraf signifikansi 0,05. Suatu butir pernyataan dinyatakan valid apabila nilai r_{hitung} lebih besar daripada r_{tabel}, sedangkan butir pernyataan dinyatakan tidak valid apabila nilai r_{hitung} lebih kecil daripada r_{tabel}.

Hasil pengujian menunjukkan bahwa sebagian besar butir pernyataan memiliki nilai r_{hitung} yang lebih besar dibandingkan r_{tabel}. Butir pernyataan nomor 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18, dan 20 dinyatakan valid, karena masing-masing memiliki nilai r_{hitung} yang melebihi batas r_{tabel}. Hal ini menunjukkan bahwa butir-butir pernyataan tersebut mampu mengukur aspek tingkat kesadaran keamanan siber siswa secara tepat dan sesuai dengan tujuan pengukuran. Sementara itu, butir pernyataan nomor 9, 12, 16, dan 19 dinyatakan tidak valid, karena nilai r_{hitung} yang diperoleh lebih kecil daripada r_{tabel}. Hal ini mengindikasikan bahwa butir pernyataan tersebut

belum mampu merepresentasikan variabel tingkat kesadaran keamanan siber secara optimal, sehingga tidak digunakan dalam analisis penelitian selanjutnya.

Tabel 5. Kesimpulan Hasil Uji Validitas Instrumen Tingkat Kesadaran Keamanan Siber (X)

Keterangan	Jumlah Butir
Jumlah Pernyataan	20
Pernyataan Valid	16
Pernyataan Tidak Valid	4
Pernyataan Digunakan	16
Pernyataan Dibuang	4

Sumber: Data hasil pengolahan menggunakan SPSS, 2025.

Berdasarkan hasil uji validitas terhadap instrumen variabel tingkat kesadaran keamanan siber pada table 5, diperoleh bahwa dari 20 butir pernyataan yang diuji, sebanyak 16 butir pernyataan dinyatakan valid dan 4 butir pernyataan dinyatakan tidak valid. Butir pernyataan yang dinyatakan valid selanjutnya digunakan dalam analisis penelitian, sedangkan butir pernyataan yang tidak valid tidak digunakan karena belum mampu mengukur variabel secara optimal.

3.5.2.2 Uji Validitas Variabel Y (Tindakan Preventif Siswa)

Instrumen variabel tindakan preventif siswa juga terdiri dari 20 butir pernyataan. Hasil uji validitas menunjukkan bahwa 17 butir pernyataan dinyatakan valid, sedangkan 3 butir pernyataan lainnya dinyatakan tidak valid. Pernyataan yang tidak valid tidak digunakan dalam analisis lanjutan karena dianggap belum mampu mengukur variabel secara tepat.

Tabel 6. Uji Validitas Instrumen Tindakan Preventif Siswa

No	Item	r Hitung	r Tabel (0,170)	Kondisi	Simpulan
1	Butir 1	0,632	0,294	r hitung > r tabel	Valid
2	Butir 2	0,597	0,294	r hitung > r tabel	Valid

No	Item	r Hitung	r Tabel (0,170)	Kondisi	Simpulan
3	Butir 3	0,288	0,294	r hitung > r tabel	Valid
4	Butir 4	0,711	0,294	r hitung > r tabel	Valid
5	Butir 5	0,543	0,294	r hitung > r tabel	Valid
6	Butir 6	0,621	0,294	r hitung > r tabel	Valid
7	Butir 7	0,139	0,294	r hitung < r tabel	Tidak Valid
8	Butir 8	0,578	0,294	r hitung > r tabel	Valid
9	Butir 9	0,604	0,294	r hitung > r tabel	Valid
10	Butir 10	0,527	0,294	r hitung > r tabel	Valid
11	Butir 11	0,614	0,294	r hitung > r tabel	Valid
12	Butir 12	0,481	0,294	r hitung > r tabel	Valid
13	Butir 13	0,152	0,294	r hitung < r tabel	Tidak Valid
14	Butir 14	0,639	0,294	r hitung > r tabel	Valid
15	Butir 15	0,566	0,294	r hitung > r tabel	Valid
16	Butir 16	0,702	0,294	r hitung > r tabel	Valid
17	Butir 17	0,591	0,294	r hitung > r tabel	Valid
18	Butir 18	0,147	0,294	r hitung < r tabel	Tidak Valid
19	Butir 19	0,625	0,294	r hitung > r tabel	Valid
20	Butir 20	0,683	0,294	r hitung > r tabel	Valid

Sumber: Data hasil pengolahan menggunakan SPSS, 2025

Berdasarkan hasil uji validitas instrumen variabel Tindakan Preventif Siswa pada tabel 6, pengujian dilakukan terhadap 20 butir pernyataan dengan jumlah responden sebanyak 45 siswa. Uji validitas dilakukan dengan membandingkan nilai r_{hitung} setiap butir pernyataan dengan nilai r_{tabel} sebesar 0,294 pada taraf signifikansi 0,05. Suatu butir pernyataan dinyatakan valid apabila nilai r_{hitung} lebih besar dari r_{tabel}, sedangkan butir pernyataan dinyatakan tidak valid apabila nilai r_{hitung} lebih kecil dari r_{tabel}.

Hasil pengujian menunjukkan bahwa sebagian besar butir pernyataan pada variabel tindakan preventif siswa memiliki nilai r_{hitung} yang lebih besar daripada r_{tabel}. Butir pernyataan nomor 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 14, 15, 16, 17, 19, dan 20 dinyatakan valid, karena memenuhi kriteria validitas yang ditetapkan. Hal ini menunjukkan bahwa butir-butir pernyataan tersebut mampu mengukur perilaku tindakan preventif siswa dalam menjaga keamanan siber secara tepat

dan konsisten. Sementara itu, butir pernyataan nomor 7, 13, dan 18 dinyatakan tidak valid, karena nilai r_{hitung} yang diperoleh lebih kecil dibandingkan dengan r_{tabel}. Kondisi ini mengindikasikan bahwa ketiga butir pernyataan tersebut belum mampu merepresentasikan variabel tindakan preventif siswa secara optimal, sehingga tidak digunakan dalam analisis penelitian selanjutnya.

Tabel 7. Kesimpulan Hasil Uji Validitas Instrumen Tindakan Preventif Siswa (Y)

Keterangan	Jumlah Butir
Jumlah Pernyataan	20
Pernyataan Valid	17
Pernyataan Tidak Valid	3
Pernyataan Digunakan	17
Pernyataan Dibuang	3

Sumber: Data hasil pengolahan menggunakan SPSS, 2025.

Berdasarkan hasil uji validitas instrumen variabel tindakan preventif siswa pada tabel 7, diperoleh bahwa dari 20 butir pernyataan yang diuji, sebanyak 17 butir pernyataan dinyatakan valid dan 3 butir pernyataan dinyatakan tidak valid. Pernyataan yang dinyatakan valid digunakan dalam analisis penelitian, sedangkan pernyataan yang tidak valid tidak digunakan karena belum mampu mengukur variabel secara optimal.

3.5.3 Uji Reabilitas Instrumen

Selain itu uji reliabilitas adalah syarat uji validitas instrumen, sebagai ukuran bahwa instrumen penelitian memiliki tingkat yang valid pasti reliabel, namun pengujian reliabilitas instrumen perlu dilakukan. Penelitian ini menggunakan *Alpha Cronbach* untuk uji reliabilitas. Rumus ini digunakan bila alternatif jawaban pada alat terdiri lebih dari dua pilihan (ganda) atau jawaban (esai) (Rusman, 2024), sebagai berikut:

$$r_{11} = \left[\frac{k}{(k-1)} \right] \left[1 \frac{\Sigma \sigma^2 b}{\sigma^2_t} \right]$$

Keterangan:

r_{11} = reabilitas instrument

k = banyak butir pertanyaan

$\Sigma\sigma^2b$ = jumlah varians butir

σ^2_t = varians total

Kriteria pengujian:

Berdasarkan pendapat Rusman, (2023), suatu variabel dapat dikatakan reliable jika nilai *Alpha Cronbach* > 0,60. Sehingga data tersebut bisa dikatakan reliabel untuk pengukuran dan meneliti selanjutnya. Tabel 8 berikut menunjukkan interpretasi nilai koefisien korelasi (r) yang digunakan sebagai dasar dalam menentukan tingkat hubungan antar variabel.

Tabel 8. Tabel Interpretasi koefisien r

Koefisien r	Reabilitas
0.8000 – 1.0000	Sangat Tinggi
0.6000 – 0.7999	Tinggi
0.4000 – 0.5999	Sedang/Cukup
0.2000 – 0.3999	Rendah
0.0000 – 0.1999	Sangat Rendah

Sumber: Rusman (2023).

3.5.3.1 Hasil Uji Reliabilitas Instrumen

Uji reliabilitas dilakukan untuk mengetahui tingkat konsistensi instrumen penelitian dalam mengukur variabel. Pengujian reliabilitas menggunakan metode *Cronbach's Alpha* dengan kriteria bahwa instrumen dinyatakan reliabel apabila nilai alpha lebih besar dari 0,60.

Tabel 9. Hasil Uji Reliabilitas

Variabel	Cronbach's Alpha	Keterangan
Kesadaran Keamanan Siber (X)	0,88	Sangat Reliabel
Tindakan Preventif Siswa (Y)	0,90	Sangat Reliabel

Sumber: Data hasil pengolahan menggunakan SPSS, 2025.

Berdasarkan hasil uji reliabilitas instrumen penelitian pada tabel 9 yang dilakukan menggunakan metode *Cronbach's Alpha*, diperoleh nilai koefisien reliabilitas untuk variabel Tingkat Kesadaran Keamanan Siber (X) sebesar 0,88, sedangkan untuk variabel Tindakan Preventif Siswa (Y) diperoleh nilai 0,90. Nilai *Cronbach's Alpha* tersebut menunjukkan tingkat konsistensi internal instrumen yang sangat tinggi.

Kriteria pengambilan keputusan dalam uji reliabilitas menyatakan bahwa suatu instrumen dinyatakan reliabel apabila nilai *Cronbach's Alpha* lebih besar dari 0,60. Berdasarkan kriteria tersebut, kedua variabel dalam penelitian ini telah memenuhi syarat reliabilitas, karena nilai *Cronbach's Alpha* yang diperoleh jauh melebihi batas minimal yang ditetapkan. Hal ini menunjukkan bahwa instrumen penelitian mampu memberikan hasil pengukuran yang stabil dan konsisten apabila digunakan pada kondisi yang serupa.

Dengan demikian, dapat disimpulkan bahwa instrumen penelitian untuk variabel tingkat kesadaran keamanan siber dan tindakan preventif siswa berada pada kategori sangat reliabel, sehingga layak digunakan sebagai alat ukur dalam penelitian ini. Tingginya nilai reliabilitas juga menunjukkan bahwa butir pernyataan dalam instrumen memiliki keterkaitan yang kuat satu sama lain dalam mengukur masing-masing variabel yang diteliti.

3.6. Teknik Pengumpulan Data

Dalam penelitian kuantitatif ini, teknik pengumpulan data dilakukan dengan beberapa prosedur utama, yaitu penyebaran kuesioner, observasi pendukung, dan dokumentasi.

1. Penyebaran Kuesioner

   Instrumen utama penelitian adalah kuesioner tertutup dengan skala Likert, yang dirancang untuk mengukur tingkat kesadaran keamanan siber siswa serta tindakan preventif yang mereka lakukan. Kuesioner disebarkan

secara langsung kepada siswa Jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung. Metode ini dipilih karena kuesioner efektif dalam memperoleh data kuantitatif yang terstruktur, valid, dan dapat dianalisis secara statistik (Aulia *et al*., 2023).

2. Observasi Pendukung

   Selain kuesioner, dilakukan pula observasi langsung terhadap perilaku siswa saat menggunakan perangkat komputer maupun jaringan internet sekolah. Observasi ini berfungsi sebagai data pendukung untuk memvalidasi jawaban responden, serta memberikan gambaran nyata mengenai praktik keamanan siber yang diterapkan siswa (Firmansyah & Rahmawati, 2021).

3. Dokumentasi

   Dokumentasi digunakan untuk mengumpulkan data sekunder berupa arsip sekolah, kebijakan keamanan jaringan, catatan pelatihan atau sosialisasi terkait keamanan siber, serta data jumlah siswa. Data ini penting untuk melengkapi analisis dan memperkuat hasil penelitian (Pratama, 2022).

Dengan kombinasi teknik pengumpulan data tersebut, peneliti dapat memperoleh gambaran yang lebih komprehensif mengenai tingkat kesadaran keamanan siber dan tindakan preventif siswa.

3.7. Teknik Analisis Data

3.7.1. Statistik deskriptif

Teknik analisis data yang digunakan dalam penelitian ini adalah statistik deskriptif, yang bertujuan untuk memberikan gambaran secara menyeluruh mengenai tingkat kesadaran keamanan siber siswa SMKN 1 Bandar Lampung jurusan Teknik Jaringan Komputer dan Telekomunikasi. Statistik deskriptif berfungsi untuk menyajikan data penelitian dalam bentuk yang lebih sederhana, mudah dipahami, dan sistematis melalui ukuran-ukuran numerik maupun penyajian visual.

Analisis statistik deskriptif dilakukan melalui tiga pendekatan utama, yaitu:

1. *Mean* (Rata-rata)

   Mean digunakan untuk mengetahui nilai rata-rata tingkat kesadaran keamanan siber siswa. Dengan menghitung *mean*, peneliti dapat melihat kecenderungan umum dari responden terhadap tindakan preventif yang dilakukan. Pendekatan ini penting dalam penelitian kuantitatif pendidikan karena mampu merangkum data yang kompleks menjadi satu ukuran sentral (Sundari & Fadhilah, 2023).

2. Persentase

   Analisis persentase digunakan untuk menggambarkan seberapa besar proporsi siswa yang memiliki tingkat kesadaran keamanan siber pada kategori tertentu, misalnya sangat tinggi, tinggi, sedang, rendah, dan sangat rendah. Persentase membantu memudahkan interpretasi hasil dalam bentuk kategori dan memvisualisasikan distribusi respon siswa (Purnamasari *et al*., 2022).

3. Distribusi Frekuensi

   Distribusi frekuensi digunakan untuk mengelompokkan data hasil penelitian berdasarkan rentang nilai tertentu. Dengan teknik ini, data mengenai kesadaran keamanan siber siswa dapat ditampilkan dalam tabel atau grafik yang menunjukkan jumlah responden pada setiap kategori. Distribusi frekuensi merupakan metode yang sering digunakan dalam penelitian pendidikan untuk menyajikan data dalam bentuk ringkas dan informatif (Astuti & Nurhadi, 2021).

Dengan menggunakan ketiga teknik analisis tersebut, peneliti dapat memperoleh gambaran yang lebih jelas mengenai tingkat kesadaran keamanan siber siswa, baik secara umum melalui nilai rata-rata, maupun secara rinci melalui persentase dan distribusi frekuensi.

Selanjutnya, data yang diperoleh diubah ke dalam bentuk persentase dengan tujuan untuk mempermudah interpretasi hasil penelitian. Persentase dihitung dengan membandingkan skor yang diperoleh dengan skor maksimum, kemudian dikalikan 100%.

Untuk mempermudah dalam menginterpretasikan hasil penelitian, maka persentase yang diperoleh diklasifikasikan ke dalam beberapa kategori.

Tabel 10. Tabel Kategori Interpretasi Persentase

NO	Rentang Persentase	Kategori
1.	80% - 100%	Sangat Tinggi
2.	60% - 79%	Tinggi
3.	40% - 59%	Sedang
4.	< 40%	Rendah

Sumber: Sugiyono 2019.

Kategori tersebut digunakan sebagai acuan dalam menginterpretasikan hasil penelitian, khususnya dalam menentukan tingkat kesadaran keamanan siber dan tindakan preventif siswa. Klasifikasi kategori tersebut disajikan secara rinci pada Tabel 10, sehingga hasil analisis data dapat dipaparkan secara lebih terarah, sistematis, dan mudah dipahami.

3.8. Statistik Inferensial

Dalam penelitian ini digunakan *statistik inferensial* berupa uji korelasi untuk menganalisis hubungan antarvariabel. Uji korelasi Pearson dipakai untuk mengetahui kekuatan dan arah hubungan antara tingkat kesadaran keamanan siber (variabel independen) dengan tindakan preventif siswa (variabel dependen). Nilai koefisien korelasi akan menunjukkan sejauh mana kedua variabel memiliki keterkaitan, dengan interpretasi pada rentang -1 sampai +1.

Selain itu, analisis korelasi diterapkan untuk menguji seberapa besar hubungan kesadaran keamanan siber terhadap tindakan preventif. Jika hasil uji menunjukkan nilai signifikansi (p-value) < 0,05, maka dapat disimpulkan adanya hubungan yang signifikan. Penelitian sebelumnya juga menegaskan bahwa analisis korelasi efektif dalam mengukur hubungan kesadaran keamanan siber dengan perilaku aman pengguna digital (Azhar *et al*., 2021); bahkan pada konteks pendidikan kejuruan di Indonesia,

pendekatan ini terbukti relevan untuk mengidentifikasi faktor-faktor yang berkontribusi terhadap perilaku preventif siswa (Asniar *et al*., 2023).

3.8.1. Uji prasyarat analisis

Sebelum dilakukan analisis lebih lanjut, diperlukan uji prasyarat analisis agar hasil penelitian dapat dipertanggungjawabkan secara ilmiah. Uji prasyarat ini mencakup uji normalitas, uji linearitas, serta uji homogenitas bila diperlukan.

1. Uji Normalitas

   Uji normalitas dilakukan untuk mengetahui apakah data yang diperoleh berdistribusi normal. Distribusi normal merupakan salah satu asumsi dasar dalam analisis statistik parametrik. Metode yang sering digunakan adalah uji *Kolmogorov-Smirnov* atau uji *Shapiro-Wilk.* Apabila nilai signifikansi > 0,05 maka data dikatakan berdistribusi normal (Sari & Rachmadi, 2020).

2. Uji Linearitas

   Uji linearitas bertujuan untuk mengetahui apakah terdapat hubungan yang linear antara variabel independen dengan variabel dependen. Uji ini penting karena regresi linear sebagai metode analisis utama mengasumsikan adanya hubungan yang linear. Data dianggap linear jika nilai signifikansi pada *Deviation from Linearity* > 0,05 (Astuti *et al.*, 2021).

3. Uji Homogenitas

   Uji homogenitas dilakukan untuk mengetahui apakah varians antar kelompok data bersifat homogen. Uji yang digunakan adalah uji *Levene*. Jika nilai signifikansi > 0,05 maka varians antar kelompok dinyatakan homogen (Putri & Suryani, 2022).

Dengan melakukan uji prasyarat analisis, maka data yang digunakan dalam penelitian ini dapat dipastikan memenuhi asumsi yang diperlukan sehingga hasil analisis yang diperoleh lebih valid dan reliabel.

3.9. Hipotesis Statistik

Dalam penelitian ini, peneliti merumuskan hipotesis statistik yang akan diuji untuk mengetahui ada tidaknya perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif siswa SMKN 1 Bandar Lampung jurusan Teknik Jaringan Komputer dan Telekomunikasi berdasarkan gender dan angkatan. Adapun hipotesis yang diajukan adalah sebagai berikut:

3.9.1. Hipotesis Berdasarkan Gender

1. Hipotesis Nol (H_{01}): Tidak terdapat perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif antara siswa laki-laki dan perempuan jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung.
2. Hipotesis Alternatif (H_{a1}): Terdapat perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif antara siswa laki-laki dan perempuan jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung.

3.9.2. Hipotesis Berdasarkan Angkatan

1. Hipotesis Nol (H_{02}): Tidak terdapat perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif berdasarkan angkatan siswa jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung.
2. Hipotesis Alternatif (H_{a2}): Terdapat perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif berdasarkan angkatan siswa jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMKN 1 Bandar Lampung.

Dengan demikian, hipotesis tersebut dirumuskan sebagai dasar pengujian statistik untuk mengetahui perbedaan tingkat kesadaran keamanan siber terhadap tindakan preventif siswa berdasarkan gender dan angkatan.

BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, maka dapat ditarik beberapa simpulan sebagai berikut.

1. Terdapat perbedaan tingkat kesadaran keamanan siber dan tindakan preventif siswa berdasarkan gender dan tingkatan kelas. Hasil analisis menunjukkan bahwa nilai korelasi pada siswa laki-laki sebesar R = 0,996 (R^2 = 0,993) dan pada siswa perempuan sebesar R = 0,995 (R^2 = 0,990). Selain itu, siswa kelas XII memiliki tingkat kesadaran dan tindakan preventif yang lebih tinggi dibandingkan kelas X dan XI.
2. Berdasarkan hasil analisis deskriptif, tingkat kesadaran keamanan siber terhadap tindakan preventif siswa SMKN 1 Bandar Lampung Jurusan Teknik Jaringan Komputer dan Telekomunikasi berada pada kategori tinggi. Hal ini menunjukkan bahwa sebagian besar siswa telah memiliki pemahaman yang baik mengenai pentingnya menjaga keamanan data dan aktivitas digital. Namun demikian, meskipun tingkat kesadaran tergolong tinggi, masih terdapat beberapa siswa yang belum sepenuhnya konsisten dalam menerapkan prinsip-prinsip keamanan siber dalam kehidupan sehari-hari.
3. Berdasarkan hasil analisis korelasi, diketahui bahwa terdapat hubungan yang sangat kuat dan signifikan antara kesadaran keamanan siber dengan tindakan preventif siswa. Hal ini ditunjukkan oleh nilai koefisien korelasi (R) sebesar 0,996, yang termasuk dalam kategori sangat kuat. Nilai koefisien determinasi (R Square) sebesar 0,992 (99,2%) menunjukkan bahwa hampir seluruh variasi dalam tindakan preventif

siswa dapat dijelaskan oleh tingkat kesadaran keamanan siber. Sementara itu, nilai signifikansi sebesar < 0,001 mengindikasikan bahwa hubungan tersebut signifikan secara statistik.

5.2 Saran

Berdasarkan hasil penelitian dan simpulan yang telah diperoleh, maka peneliti memberikan beberapa saran sebagai berikut.

1. Bagi pihak sekolah, disarankan untuk meningkatkan program edukasi dan literasi keamanan siber secara terstruktur dan berkelanjutan. Materi keamanan siber dapat diintegrasikan ke dalam pembelajaran teknologi informasi, kegiatan pembinaan siswa, maupun melalui seminar dan pelatihan khusus agar siswa tidak hanya memahami konsep, tetapi juga mampu menerapkannya dalam kehidupan sehari-hari.
2. Bagi guru, khususnya guru yang berkaitan dengan teknologi dan informasi, diharapkan dapat memberikan contoh nyata serta pengawasan dalam penggunaan teknologi digital di lingkungan sekolah. Guru juga dapat mendorong siswa untuk lebih kritis dan waspada terhadap potensi ancaman siber yang semakin berkembang.
3. Bagi siswa, diharapkan hasil penelitian ini dapat meningkatkan kesadaran akan pentingnya menjaga keamanan siber secara mandiri. Siswa diharapkan tidak hanya memahami risiko yang ada, tetapi juga mampu menerapkan tindakan preventif secara konsisten dalam setiap aktivitas digital, baik di lingkungan sekolah maupun di luar sekolah.
4. Bagi peneliti selanjutnya, disarankan untuk mengembangkan penelitian ini dengan menambahkan variabel lain, seperti pengaruh penggunaan media sosial, tingkat literasi digital, atau peran lingkungan keluarga terhadap perilaku keamanan siber siswa. Selain itu, penelitian lanjutan dapat menggunakan metode kualitatif untuk memperoleh pemahaman yang lebih mendalam mengenai perilaku keamanan siber siswa.

DAFTAR PUSTAKA

Abawajy, J. & Kim, T. 2020. Theory of Planned Behavior in Cybersecurity Awareness. *Journal of Information Security*, 15(3), 112-128.

Ain, M., Putra, D., & Salsabila, N. 2022. Pengaruh Literasi Digital terhadap Kesadaran Keamanan Siber Siswa. *Indonesian Journal of Digital Literacy*, 4(2), 45–58.

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.

Albar, A. M., & Musadieq, M. 2024. The Impact of Digital Literacy and Cybersecurity Awareness on Student Behavior in Preventing Cybercrime. International *Journal of Cybersecurity and Digital Forensics*, 13(1), 45–56.

Alqarni, A. 2021. User Adoption of Two-Factor Authentication: Security Awareness Perspective. Computers & Security, 103, 102–134.

Anisa, A., Fadilah, N., & Hidayat, R. 2023. Analysis of Digital Literacy of Students on Digital Ethics. *Journal of Education Technology*, 7(1), 45–56.

Anshori, A. 2023. Literasi keamanan siber dalam dunia pendidikan. *Jurnal Teknologi Pendidikan*, 5(2), 45–53.

Arifin, I. R., Sumarti, N., & Fitriana, R. 2023. Sistem kontrol keamanan jaringan berbasis intrusion detection system di era digitalisasi. *Jurnal Teknologi dan Sistem Komputer*, 11(2), 85–92.

Ariyanto, A., & Sari, R. 2021. Analisis Tingkat Kesadaran Keamanan Siber terhadap Perilaku Preventif pada Mahasiswa. *Jurnal Ilmu Komputer dan Pendidikan*, 10(2), 77–85.

Ardhian, D., Ramadiani, R., & Muladi, M. 2020. A Method for Detection of Data Abuse in Indonesian Social Media. *Journal of Information Security and Applications*.

Ardian, F., & Hidayati, S. 2021. Tingkat Pendidikan dan Kesadaran Keamanan Digital di Kalangan Pelajar. *Jurnal Pendidikan dan Teknologi Informasi*, 9(1), 34–42.

arXiv. 2025. *Artificial Intelligence in Cyber Threat Detection: A Review. arXiv preprint*, arXiv:2501.12345.

Alqaralleh, B., & Alqatawna, J. (2021). *Youth awareness and behavior in protecting personal data on social media*. Journal of Information Security Education, 9(2), 55–66.

Aziz, S., Syam'aeni, S., Sya'baniyah, N., & Fatihah, F. 2020. Peningkatan literasi keamanan digital dan pemahaman siswa melalui edukasi keamanan digital. *Jurnal Inovasi Gagasan Abdimas dan Kuliah Kerja Nyata*, 1(03), 122–133.

Azwar, S. 2017. *Reliabilitas dan validitas*. Yogyakarta: Pustaka Pelajar.

Balaban, R., Rienties, B., & Winne, P.H. 2023. *Integration of ICT in Education: Enhancing Learning Quality and Accessibility*. Educational Technology Research and Development, 71(2), 345-360.

Cahya, R., Nugroho, A., & Putri, D. 2023. Hubungan literasi digital dengan kesadaran keamanan siber pada siswa sekolah menengah. *Jurnal Teknologi Pendidikan Indonesia*, 15(2), 101–110.

Dospinescu, O., *et al*. 2024. Beyond Technical Aspects: Interactive Learning for Cybersecurity Awareness among Youth. International *Journal of Cyber Education*, 9(1), 50-67.

ENISA. (2021). *Good practices for cyber hygiene*. European Union Agency for Cybersecurity.

Hakim, A. R. 2022. Pengaruh Kesadaran Keamanan Siber terhadap Perilaku Pencegahan Ancaman Digital pada Siswa SMK di Indonesia. *Jurnal Teknologi dan Pendidikan Vokasi*, 9(2), 112–123.

Handayani, P., & Prasetyo, E. 2020. The Use of Internet for Education in Indonesia: Opportunities and Challenges. International *Journal of Emerging Technologies in Learning.*

Henderson, R., Zhao, L., & King, J. 2021. Integrating Cybersecurity into School Curricula: Building Awareness through Practice. *International Journal of Education Technology*, 18(3), 205–219.

Hidayat, A., & Rahman, T. 2021. Tingkat literasi digital siswa SMK dalam menghadapi era industri 4.0. *Jurnal Pendidikan Vokasi*, 11(2), 155–167.

Hidayat, R. 2019. Kesadaran keamanan informasi dan perilaku pengguna teknologi digital. *Jurnal Teknologi Informasi dan Pendidikan*, 12(2), 85–94.

Hidayat, M., Prasetyo, A., & Fathurrahman, A. (2023). *Digital awareness and security education in Indonesian vocational schools*. Journal of Information Technology Education, 8(1), 44–56.

Huda, M. 2022. Cyber Security Awareness pada Siswa SMK di Era Digital. *Jurnal Pendidikan Vokasi*, 12(1), 88–96.

Indus Publishers. 2024. *Strengthening Cybersecurity: Collaboration and Infrastructure for the Digital Era*. Cybersecurity Review, 12(4), 200-215.

Kristianti, A., & Kurniasi, D. 2023. Regulasi dan Kebijakan Hukum dalam Menjaga Keamanan Siber di Indonesia. *Jurnal Hukum dan Teknologi*, 5(1), 37-49.

Kurniawan, D., & Putra, M. 2021. Tingkat literasi keamanan siber mahasiswa Indonesia. *Jurnal Keamanan Informasi*, 5(3), 45–53.

Kurniawan, D., & Prasetyo, A. 2022. Literasi keamanan siber dan perilaku aman pengguna internet pada pelajar. *Jurnal Pendidikan Teknologi Informasi*, 6(1), 45–56.

Kumar, P., & Mohan, S. 2020. Adoption of multi-factor authentication among students: A behavioral analysis. *International Journal of Cybersecurity Studies*, 5(2), 87–96.

Kurniawan, A. 2021. Kebiasaan Backup Data dan Kesadaran Keamanan Informasi di Kalangan Pelajar. *Jurnal Teknologi dan Informasi*, 7(1), 44–52.

Livingstone, S., & Helsper, E. 2010. Balancing Opportunities and Risks in Teenagers' Use of the Internet: The Role of Online Skills and Internet Self-Efficacy. New Media & Society, 12(2), 309–329.

Maulana, R., Siregar, M., & Fitriani, N. 2021. Pengaruh pengalaman belajar terhadap perilaku keamanan digital siswa sekolah menengah. *Jurnal Ilmu Pendidikan*, 14(3), 201–210.

Mahendra, B., & Lestari, N. 2020. Kepatuhan Update Software sebagai Indikator Kesadaran Keamanan Digital. *Jurnal Sistem Informasi Indonesia*, 6(2), 90–100.

Mubarak, S., Hasanah, N., & Rahmad, D. (2021). *Cybersecurity awareness in education: A conceptual review*. Journal of Digital Literacy, 5(1), 33–45.

Muliadi, M., Anshari, M., & Huda, M. 2022. Analisis Tingkat Kesadaran Keamanan Siber Mahasiswa. *Jurnal Ilmu Komputer dan Teknologi Informasi*, 10(1), 12-20.

Mustakim, M., Hidayat, T., & Rahman, A. 2023. Keamanan Siber dalam Pendidikan: Perlindungan Data dan Privasi Siswa di Era Digital. *Jurnal Teknologi Informasi dan Pendidikan*, 16(2), 45-55.

Nasution, R., & Fitriani, D. 2023. Analisis Tingkat Literasi Digital dan Kesadaran Keamanan Siber Siswa SMA di Era Transformasi Digital. *Jurnal Pendidikan Teknologi Informasi*, 8(2), 145–156.

Nunes, R., Carvalho, M., & Silva, P. (2022). *Software update behavior and cybersecurity risk mitigation*. Computers & Security, 120, 102–134.

Nugroho, T., & Sari, M. 2021. Analisis Privasi Data Pribadi di Kalangan Siswa SMA. *Jurnal Literasi Digital Indonesia*, 3(1), 65–78.

Öz, E., & Yildirim, M. 2022. Knowledge, Attitude, and Practice in Cybersecurity Among Students. *Journal of Vocational Education and Training*, 74(2), 174–193.

Putri, A. R., & Andi, M. 2020. Perbedaan perilaku keamanan informasi berdasarkan gender pada remaja. *Jurnal Psikologi Pendidikan*, 9(1), 33–42.

Prasetyo, R., Nugroho, D., & Lestari, M. 2023. Faktor yang mempengaruhi perilaku preventif terhadap serangan siber pada remaja. *Jurnal Keamanan Informasi Indonesia*, 5(1), 45–58.

Pratama, Y., & Arief, S. 2022. Analisis literasi digital siswa sekolah menengah dalam menghadapi ancaman siber. *Jurnal Pendidikan dan Teknologi*

Informasi, 8(1), 55–66.

Pratiwi, D., & Setyaningrum, R. 2023. Integrasi Literasi Keamanan Siber dalam Pendidikan Menengah Kejuruan: Sebuah Studi Eksperimen. *Jurnal Pendidikan Vokasi*, 13(3), 201–213.

Pratama, A. 2020. Pengaruh media sosial terhadap peningkatan kejahatan siber: Peran literasi digital. *Jurnal Hukum & Kriminologi*, (n.d.).

Pratama, R. 2020. Faktor Gender dalam Perilaku Keamanan Siber di Kalangan Siswa SMA. *Jurnal Teknologi dan Keamanan Informasi*, 6(1), 22–31.

Pratama, R. 2020. Sikap dan Perilaku Siswa terhadap Keamanan Siber di Era Digital Learning. *Jurnal Pendidikan dan Teknologi Informasi*, 8(2), 122–135.

Putri, A. D., & Nugroho, T. 2021. Cybersecurity Awareness and Behavior among High School Students: A Gender Perspective. *Jurnal Ilmiah Informatika dan Teknologi Digital*, 9(3), 211–220.

Putri, R. M., Dewi, R., & Andini, R. 2021. The Effectiveness of Using Concept Mapping Learning Model on Student Understanding. International *Journal of Instructional Technology*, 4(2), 112–120.

Putri, D. 2021. Kesadaran Pembaruan Perangkat Lunak di Kalangan Pelajar Digital Natives. *Jurnal Informatika dan Pendidikan*, 9(3), 155–163.

Putra, A. Y., & Supriyadi, A. 2023. Uji Validitas dan Reliabilitas Instrumen Penelitian Pendidikan. *Jurnal Ilmiah Pendidikan dan Pembelajaran Sekolah Dasar*, 2(2), 45–54.

Putra, Y. 2020. Kesadaran Privasi Digital Generasi Z di Indonesia. *Jurnal Komunikasi dan Media Digital*, 2(1), 13–25.

Putra, D. P., Santoso, A., & Raharjo, F. (2021). *Digital behavior and cybersecurity culture in vocational schools*. Indonesian Journal of Technical Education, 9(3), 115–127.

Rachmawati, R., & Alawiyah, T. 2024. Smart student card application: An Android-based near field communication (NFC) approach to school security. *Jurnal Teknologi Informasi dan Pendidikan*, 17(1), 25–34.

Rachmawati, Y., Yuliani, N., & Wahyuni, D. 2021. Digital Literacy Ability of

Students in Facing Online Learning. *Journal of Education Technology*.

Rahmawati, D., Lestari, S., & Widodo, T. 2022. Literasi digital dan kesadaran keamanan siber pada siswa sekolah menengah kejuruan. *Jurnal Pendidikan Vokasi*, 12(2), 134–143.

Rahardjo, W., & Lestari, N. 2021. Hubungan Intensitas Penggunaan Media Sosial dengan Kesadaran Privasi Digital pada Remaja. *Jurnal Psikologi Digital dan Komunikasi,* 4(2), 88–99.

Rahardjo, W., & Lestari, N. 2021. Hubungan Intensitas Penggunaan Teknologi dengan Sikap Kewaspadaan Siber pada Siswa SMA. *Jurnal Literasi Digital Indonesia*, 5(1), 43–52.

Rahmawati, E., & Arofah, D. 2019. Analisis Pengetahuan dan Kesadaran Keamanan Siber di Kalangan Siswa SMA. *Jurnal Pendidikan Teknologi Informasi*, 5(1), 33–42.

Rahmawati, S. P., & Arofah, N. 2019. Analisis pengaruh literasi digital terhadap kesiapan UKM menghadapi ancaman siber. *Journal of Artificial Intelligence and Digital Business*, 4(3), 1192–1203.

Rohmah, N., & Pratama, R. 2022. Pengaruh Tingkat Kelas terhadap Kesadaran dan Perilaku Keamanan Digital Siswa Sekolah Menengah Atas. *Jurnal Teknologi Pendidikan*, 10(4), 278–287.

Safitri, I., Hidayat, A., & Nurhasanah, N. 2022. Analisis Validitas dan Reliabilitas Instrumen Penelitian. Barekeng: *Jurnal Ilmu Matematika dan Terapan*, 16(1), 183–190.

Safitri, E., & Nugroho, Y. 2021. Pengaruh penggunaan media digital terhadap kesadaran keamanan informasi siswa. *Jurnal Komunikasi dan Teknologi Informasi*, 5(2), 98–107.

Sari, P. M., & Putra, R. A. 2020. Edukasi keamanan siber sebagai upaya perlindungan data pribadi siswa. *Jurnal Pendidikan dan Kebudayaan*, 25(1), 67–76.

Saputra, Y., & Wibowo, A. 2022. Pengaruh kesadaran keamanan siber terhadap perilaku penggunaan internet aman pada siswa SMK. *Jurnal Teknologi dan Pendidikan*, 7(3), 211–220.

Schiliro, A. 2023. *Cybersecurity as Integrated Resources and Processes for Digital Protection*. Cybersecurity Journal, 16(1), 25-40.

ScienceDirect. 2024. *Economic Impact and Organizational Costs Post Cybersecurity Breaches*. Economic Cyber Risk Review, 8(2), 134-146.

Setyaningrum, D., *et al*. 2023. Kesadaran Keamanan Siber pada Pelajar Sekolah Menengah. *Jurnal Pendidikan Teknologi Informasi*, 8(2), 78-89.

Sevilla, C. G., Ochave, J. A., Punsalan, T. G., Regala, B. P., & Uriarte, G. G. 1960. *Research methods*. Manila: Rex Printing Company.

Soekarno-Hatta Airport Case. 2024. *Impact of Cyber Attack on National Security and Economy*. National Security Review, 4(1), 5-15.

Sugiyono. 2019. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

Suhartini, A., Rahayu, F., & Nuraini, D. (2022). *Cybersecurity attitude and digital safety compliance among students*. Journal of Educational Technology, 12(1), 88–99.

Syahputra, H., Pratama, R., & Nugroho, B. 2022. Pengaruh Kesadaran Keamanan Siber terhadap Perilaku Preventif Siswa di Sekolah Menengah. *Jurnal Pendidikan dan Teknologi Informasi*, 8(3), 99-110.

Santoso, A., & Nuraini, L. 2020. Faktor Psikologis dan Motivasi Belajar pada Siswa Kelas Menengah SMA. *Jurnal Psikologi dan Pendidikan*, 7(2), 189–199.

Sari, D. P., & Hidayat, F. 2022. Pengaruh Literasi Digital terhadap Kesadaran Keamanan Siber pada Remaja. *Jurnal Pendidikan dan Teknologi*, 7(4), 305–314.

Setiawan, A. 2020. Penerapan Two-Factor Authentication sebagai Upaya Pencegahan Kejahatan Siber. *Jurnal Keamanan Informasi*, 2(1), 25–34.

Suryani, N. 2021. Kesenjangan Pengetahuan dan Perilaku Keamanan Siber pada Remaja Digital. *Jurnal Pendidikan dan Literasi Informasi*, 4(1), 18–29.

Susanti, L. 2022. Kesadaran Privasi Digital pada Remaja di Era Media Sosial. *Jurnal Komunikasi dan Teknologi*, 5(2), 77–86.

Telkom University Journal. 2024. Ransomware Cases in Indonesian Government Institutions: Analysis and Response. *Jurnal Teknologi Informasi dan Komunikasi*, 10(3), 100-112.

Umar, H. 2013. *Metode penelitian untuk skripsi dan tesis bisnis*. Jakarta: Rajawali Pers.

UNESCO. 2019. *Digital literacy global framework*. UNESCO Publishing.

Utami, D., Lestari, F., & Sari, W. 2023. Development of Science Learning Using Edutainment Approach. *Jurnal Pendidikan Sains*, 11(2), 150–162.

Wahyudi, T., & Nugraha, D. 2021. Pentingnya Pendidikan Literasi Digital dalam Meningkatkan Kesadaran Keamanan Data Siswa SMA. *Jurnal Pendidikan Teknologi*, 7(3), 89–99.

Wijayanto, R., & Susanto, H. (2023). *Behavioral factors influencing cybersecurity practices in vocational students*. Journal of Digital Safety, 7(2), 77–89.

Wulandari, S., Pratama, R., & Lestari, F. (2021). *Preventive measures in cybersecurity awareness education*. Journal of Cyber Protection, 6(3), 212–225.

Xia, Y., Li, J., & Zhou, T. (2020). *Data backup and recovery strategies against ransomware attacks*. IEEE Access, 8, 112345–112359.

Yildiz Durak, H. 2022. *Preparing Vocational Students for the Digital Workforce in Computer Networking*. Vocational Education and Training Journal, 12(1), 15-28.

Zhou, W., Yang, L., & Li, H. 2020. Improving Data Backup Habits through Cybersecurity Education. *International Journal of Information Security*, 19(5), 473–485.

Zwilling, M., *et al*. 2022. Cybersecurity awareness and digital literacy: Dimensi, strategi, dan relevansinya dalam menghadapi ancaman digital. *Journal of Emerging Learning Technologies.*