

**ANALISIS KESADARAN KEAMANAN SIBER PADA SISWA
SMP DI NGANJUK**



Disusun Oleh:

N a m a : A. Zakki Fikril Maulidi
NIM : 17523234

**PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2024**

HALAMAN PENGESAHAN DOSEN PEMBIMBING

ANALISIS KESADARAN KEAMANAN SIBER PADA SISWA
SMP DI NGANJUK

TUGAS AKHIR



Pembimbing 1,

(Fayruz Rahma, S.T., M.Eng.)

Pembimbing 2,

(Sheila Nurul Huda, S.Kom., M.Cs)

HALAMAN PENGESAHAN DOSEN PENGUJI

**ANALISIS KESADARAN KEAMANAN SIBER PADA SISWA
SMP DI NGANJUK****TUGAS AKHIR**

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 23 Agustus 2024

Tim Penguji

Sheila Nurul Huda, S.Kom., M.Cs.



Anggota 1

Chanifah Indah Ratnasari, S.Kom.,
M.Kom.



Anggota 2

Moh. Idris, S.Kom., M.Kom.



Mengetahui,

Ketua Program Studi Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia



(Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : A Zakki Fikril Maulidi

NIM : 17523234

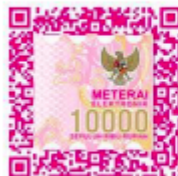
Tugas akhir dengan judul:

**ANALISIS KESADARAN KEAMANAN SIBER PADA SISWA
SMP DI NGANJUK**

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 23 Agustus 2024



(A Zakki Fikril Maulidi)

HALAMAN PERSEMBAHAN

Puji syukur kepada Allah Swt. yang telah memberikan kenikmatan, kesehatan, kemampuan, dan kekuatan, sehingga saya dapat mengerjakan tugas akhir ini hingga selesai. Selawat dan salam tetap tercurahkan kepada Nabi Muhammad saw. Semoga kita kelak mendapatkan syafaat-Nya di hari akhir nanti. Amiin.

Terima kasih saya ucapkan kepada Ibu saya dan Almarhum Bapak saya yang selalu memberikan *support* kepada saya, baik berupa motivasi, do'a, maupun *financial* untuk saya, sehingga saya bisa menyelesaikan kuliah saya. Semoga segala kebaikan yang diberikan menjadi amal yang bermanfaat dan berkah.

Tak lupa terima kasih saya sampaikan kepada dosen pembimbing saya, karena berkat dukungan beliau, saya bisa mengerjakan dan menyelesaikan tugas akhir ini. Terima kasih kepada Bu Fayruz dan Bu Sheila atas arahan, bimbingan, dan motivasi kepada saya, sehingga saya semangat untuk mengerjakan tugas akhir ini.

Terima kasih saya ucapkan kepada Program Studi Informatika – Program Sarjana, Fakultas Teknologi Industri yang telah mendukung saya dalam menjalankan tugas akhir saya hingga selesai. Ucapan terima kasih juga saya sampaikan kepada seluruh dosen dan staf Program Studi Informatika yang telah memberikan ilmu, bimbingan, serta fasilitas yang diperlukan selama masa studi.

HALAMAN MOTO

“OJO LALI TUJUANE SONGKO OMAH”

(KH. Ahmad Thohir Musthofa)

KATA PENGANTAR

Puji syukur kepada Allah Swt. yang telah memberikan kenikmatan, kesehatan, dan kekuatan, sehingga saya dapat mengerjakan tugas akhir ini hingga selesai. Selawat dan salam tetap tercurahkan kepada Nabi Muhammad saw. Semoga kita kelak mendapatkan syafaat-Nya di hari akhir nanti. Amiin.

Tugas akhir dengan judul “Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk” ini disusun sebagai salah satu persyaratan untuk kelulusan dan perolehan gelar sarjana di Jurusan Informatika Universitas Islam Indonesia. Semoga penelitian tugas akhir ini dapat memberikan manfaat bagi diri saya serta orang lain.

Terima kasih saya sampaikan sebesar-besarnya atas motivasi, do’a, dan dukungan yang telah diberikan kepada:

1. Alm. Bapak Abdul Hamid dan Ibu Dewi Asiyah yang selalu mendukung saya dalam penulisan tugas akhir ini.
2. Bapak Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D. selaku Ketua Program Studi Informatika.
3. Ibu Fayruz Rahma, S.T., M.Eng. dan Ibu Sheila Nurul Huda, S.Kom., M.Cs selaku dosen pembimbing tugas akhir saya yang telah banyak memberi arahan, bimbingan, dan motivasi kepada saya.
4. Ibu Fayruz Rahma, S.T., M.Eng. selaku dosen pembimbing akademik yang telah memberi motivasi, dukungan, dan selalu bersedia memberi arahan ketika saya berkonsultasi.
5. Seluruh dosen Program Studi Informatika yang telah membagikan ilmu dan pengalamannya selama saya kuliah.
6. Kepala SMPN 1 Ngetos dan SMP Progresif Baitul Atieq yang telah mendukung saya dalam pengisian kuesioner dalam penelitian tugas akhir ini.

Yogyakarta, 23 Agustus 2024



(A Zakki Fikril Maulidi)

SARI

Remaja, termasuk siswa SMP, merupakan pengguna internet tertinggi di Indonesia dalam beberapa tahun terakhir sehingga mereka berpeluang terkena kejahatan siber. Namun, analisis kesadaran keamanan siber umumnya lebih banyak dilakukan pada mahasiswa, karyawan, atau masyarakat umum. Sementara itu, kajian kesadaran keamanan siber yang fokus pada siswa SMP masih jarang ditemukan. Terlebih lagi, belum ada penelitian yang meneliti kesadaran keamanan siber di kalangan santri pondok pesantren yang sehari-hari jarang menggunakan gawai. Meskipun demikian, santri pondok pesantren tetap berisiko menjadi korban kejahatan siber karena mereka sesekali menggunakan gawai untuk berkomunikasi dengan orang di luar pondok. Tujuan penelitian ini untuk mengukur nilai kesadaran siswa SMP terhadap kesadaran keamanan siber berdasarkan faktor demografis, seperti gender, kelas, dan asal sekolah (negeri/pondok). Data primer diperoleh melalui survei terhadap 49 siswa SMP Negeri 1 Ngetos dan 50 siswa SMP Baitul Atieq Nganjuk. Penelitian ini mengadopsi pertanyaan dari *The Human Aspects of Information Security Questionnaire* (HAIS-Q) dan menggunakan model Kruger-Kearney untuk menganalisis data survei tersebut. Hasil analisis menunjukkan bahwa level kesadaran keamanan siber siswa SMP di Nganjuk sudah berada di level sedang, dengan total skor keseluruhan 61. Namun, skor ini mendekati level buruk. Perbedaan faktor demografis juga menghasilkan nilai kesadaran yang berbeda pada setiap dimensi dan topik yang digunakan untuk pengukuran tingkat kesadaran keamanan siber pada siswa SMP di Nganjuk.

Kata kunci: kesadaran keamanan siber, siswa SMP, HAIS-Q, Kruger-Kearney

GLOSARIUM

Data Primer	Informasi yang dikumpulkan langsung dari sumbernya melalui metode penelitian seperti survei, wawancara, atau observasi.
Demografi	Studi statistik tentang populasi manusia, termasuk analisis mengenai struktur, distribusi, dan tren mereka berdasarkan faktor-faktor seperti usia, gender, pendapatan, pendidikan, pekerjaan, dan lokasi geografis. Demografi sering digunakan untuk memahami karakteristik kelompok tertentu dalam suatu populasi dan bagaimana mereka berubah dari waktu ke waktu.
Gawai	Perangkat elektronik seperti ponsel, tablet, atau komputer yang digunakan untuk berkomunikasi dan mengakses informasi.
Generate	Kata kerja yang berarti "menghasilkan" atau "menciptakan." Istilah ini merujuk pada tindakan produksi atau penciptaan sesuatu, baik itu fisik, konseptual, atau digital.
HAIS-Q	Kuesioner yang dirancang untuk menilai aspek-aspek manusia dalam keamanan informasi, termasuk perilaku dan kesadaran individu terhadap risiko keamanan siber.
Siber	Istilah yang berkaitan dengan teknologi informasi dan komunikasi, khususnya yang berhubungan dengan internet, komputer, dan jaringan.

DAFTAR ISI

SAMPUL.....	i
HALAMAN PENGESAHAN DOSEN PEMBIMBING.....	ii
HALAMAN PENGESAHAN DOSEN PENGUJI.....	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
HALAMAN PERSEMBAHAN.....	v
HALAMAN MOTO.....	vi
KATA PENGANTAR.....	vii
SARI.....	viii
GLOSARIUM.....	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Lingkup Penelitian.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Metodologi Penelitian.....	3
1.7 Sistematika Penulisan.....	3
BAB II KAJIAN PUSTAKA.....	5
2.1 Keamanan Siber.....	5
2.1.1 Kesadaran Keamanan Siber.....	5
2.1.2 Kesadaran Keamanan Siber Pada Siswa SMP.....	6
2.1.3 Faktor-Faktor yang Memengaruhi Kesadaran Keamanan Siber.....	6
2.2 Metode untuk Mengukur Kesadaran Keamanan Siber.....	7
2.2.1 Kruger dan Kearney.....	7
2.2.2 <i>Human Aspect of Information Security Questionnaire (HAIS-Q)</i>	7
2.2.3 <i>Structural Equation Modeling (SEM)</i>	8
2.3 Kesadaran Keamanan Siber yang Harus Dipahami oleh Siswa SMP.....	8
2.3.1 Pengelolaan Kata Sandi.....	8
2.3.2 <i>Phishing Awareness</i>	8
2.3.3 <i>Internet Safety</i>	9
2.3.4 <i>Online Privacy</i>	9
2.4 Hubungan Faktor Demografis Terhadap Kesadaran Keamanan Siber.....	9
2.4.1 Kesadaran Keamanan Siber Berdasarkan Gender.....	9
2.4.2 Kesadaran Keamanan Siber Berdasarkan Kelas.....	10
2.4.3 Kesadaran Keamanan Siber Berdasarkan Asal Sekolah.....	10
2.4.4 Kesadaran Keamanan Siber Berdasarkan Uang Saku Harian.....	10
2.5 Tinjauan Pustaka.....	10
BAB III METODOLOGI PENELITIAN.....	13
3.1 Populasi.....	13
3.2 Sampel.....	13
3.3 Instrumen Penelitian.....	14
3.4 Analisis Data.....	17
BAB IV HASIL DAN PEMBAHASAN.....	22
4.1 Demografis Responden.....	22

4.1.1	Persentase Responden Berdasarkan Gender.....	23
4.1.2	Persentase Jumlah Responden Berdasarkan Kelas.....	24
4.1.3	Persentase Responden Berdasarkan Asal Sekolah.....	24
4.1.4	Persentase Responden Berdasarkan Uang Saku.....	25
4.2	Analisis Skor Kesadaran.....	26
4.2.1	Nilai Kesadaran Keseluruhan Responden.....	35
4.2.2	Nilai Kesadaran Berdasarkan Gender.....	36
4.2.3	Nilai Kesadaran Berdasarkan Kelas.....	39
4.2.4	Nilai Kesadaran Berdasarkan Asal Sekolah.....	41
4.2.5	Nilai Kesadaran Berdasarkan Uang Saku.....	43
4.3	Skor Kesadaran Keseluruhan dalam Bentuk Tabel.....	46
	BAB V KESIMPULAN DAN SARAN.....	48
5.1	Kesimpulan.....	48
5.2	Saran.....	48
	DAFTAR PUSTAKA.....	49
	LAMPIRAN.....	51

DAFTAR TABEL

Tabel 3.1 Daftar Pertanyaan	17
Tabel 3.2 Penilaian dari Kuesioner	20
Tabel 3.3 Pembobotan Dimensi	20
Tabel 3.4 Pembagian Pertanyaan untuk Setiap Topik	21
Tabel 4.1 Demografis Responden	22
Tabel 4.2 Skor Kesadaran Keseluruhan	46

DAFTAR GAMBAR

Gambar 3.1 Kerangka pengukur kesadaran keamanan siber	15
Gambar 3.2 Gambaran daftar kuesioner	16
Gambar 4.1 Persentase responden berdasarkan gender	23
Gambar 4.2 Jumlah responden berdasarkan kelas	24
Gambar 4.3 Jumlah responden berdasarkan asal sekolah	25
Gambar 4.4 Persentase uang saku responden	25
Gambar 4.5 Kumpulan jawaban kuesioner	27
Gambar 4.6 Pengolahan pertanyaan positif	27
Gambar 4.7 Pengolahan pertanyaan negatif	28
Gambar 4.8 Topik setiap dimensi masing-masing responden	29
Gambar 4.9 Nilai total pertanyaan (NTP).....	29
Gambar 4.10 Penghitungan rata-rata NTP	30
Gambar 4.11 Skor variabel Z masing-masing responden	30
Gambar 4.12 Penjumlahan variabel Z	31
Gambar 4.13 Skor kesadaran setiap topik dan dimensi	32
Gambar 4.14 Input skor berdasarkan masing-masing topik dan masing-masing dimensi	32
Gambar 4.15 Input skor semua topik	32
Gambar 4.16 Penghitungan kesadaran per dimensi (TD)	33
Gambar 4.17 Nilai kesadaran per topik	33
Gambar 4.18 Rata-rata kesadaran TD dan TP	34
Gambar 4.19 Hasil akhir skor kesadaran	34
Gambar 4.20 Nilai kesadaran keseluruhan responden	35
Gambar 4.21 Skor kesadaran keseluruhan setiap topik dan dimensi	36
Gambar 4.22 Nilai kesadaran Laki-laki	36
Gambar 4.23 Nilai kesadaran Perempuan	37
Gambar 4.24 Perbandingan skor kesadaran setiap dimensi berdasarkan gender	38
Gambar 4.25 Perbandingan skor kesadaran setiap topik berdasarkan gender	38
Gambar 4.26 Skor kesadaran kelas VII	39
Gambar 4.27 Skor kesadaran kelas VIII	39
Gambar 4.28 Skor Kesadaran kelas IX	40
Gambar 4.29 Perbandingan nilai kesadaran setiap dimensi berdasarkan kelas	40
Gambar 4.30 Perbandingan skor kesadaran setiap topik berdasarkan kelas	41

Gambar 4.31 Skor siswa SMPN 1 Ngetos	41
Gambar 4.32 Skor siswa SMP Progresif Baitul Atieq	42
Gambar 4.33 Perbandingan skor kesadaran setiap dimensi berdasarkan asal sekolah	42
Gambar 4.34 Perbandingan skor kesadaran setiap topik berdasarkan asal sekolah	43
Gambar 4.35 Skor kesadaran siswa dengan uang saku kurang dari Rp5000,00.....	43
Gambar 4.36 Skor kesadaran siswa dengan uang saku Rp5000,00 sampai Rp10.000,00.....	44
Gambar 4.37 Skor kesadaran siswa dengan uang saku lebih dari Rp10.000,00.....	44
Gambar 4.38 Perbandingan skor kesadaran setiap dimensi berdasarkan uang saku per hari ..	45
Gambar 4.39 Perbandingan skor kesadaran setiap topik berdasarkan uang saku per hari	45

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi di era digital semakin maju sehingga kesadaran keamanan siber menjadi sesuatu penting untuk diperhatikan, terutama di kalangan remaja yang semakin akrab dengan penggunaan teknologi informasi. Di Indonesia, penetrasi internet semakin meluas, termasuk di wilayah-wilayah pedesaan. Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), penggunaan internet di kalangan remaja, termasuk siswa SMP, meningkat pesat dalam beberapa tahun terakhir (Pahlevi, 2022).

Kesadaran keamanan siber merujuk pada pemahaman dan kesadaran individu terhadap ancaman, risiko, serta praktik-praktik yang dapat melindungi sistem dan informasi dari serangan atau akses yang tidak sah. Kesadaran ini mencakup pengetahuan tentang cara-cara mengidentifikasi ancaman, penggunaan kata sandi yang kuat, pengelolaan akses, hingga cara merespon insiden keamanan siber (Kruger & Kearney, 2006).

Kesadaran keamanan siber berperan penting dalam mengurangi risiko kejahatan siber. Ketika individu dan organisasi memiliki pengetahuan yang cukup tentang ancaman siber dan cara mengatasinya, mereka dapat menentukan langkah-langkah proaktif untuk mengamankan mereka. Misalnya, kesadaran tentang *phishing* dapat membantu pengguna mengenali dan menghindari pesan yang mencurigakan, sehingga mengurangi kemungkinan menjadi korban pencurian identitas atau informasi (Parsons et al., 2017).

Beberapa penelitian telah dilakukan untuk menganalisis kesadaran keamanan siber. Namun, masih jarang yang meneliti kesadaran keamanan siber di kalangan siswa SMP. Terlebih lagi, belum ada penelitian yang meneliti kesadaran keamanan siber di kalangan santri pondok pesantren yang sehari-hari jarang menggunakan gawai. Meskipun demikian, santri pondok pesantren tetap berisiko menjadi korban kejahatan siber karena mereka sesekali menggunakan gawai untuk berkomunikasi dengan orang di luar pondok.

Tujuan dari penelitian ini adalah untuk mengukur skor kesadaran terkait keamanan siber pada kalangan siswa SMP sesuai dengan faktor demografinya, seperti gender, kelas, asal sekolah, dan uang saku harian mereka. Data primer dalam penelitian ini diperoleh dengan melakukan survei terhadap siswa di SMP Negeri 1 Ngetos dan SMP Progresif Baitul Atieq Nganjuk (SMP swasta berbasis pesantren).

Penelitian ini menggunakan model Kruger-Kearney untuk menganalisis data survei tersebut. Model Kruger-Kearney adalah salah satu model yang digunakan untuk mengukur dan memahami kesadaran keamanan siber dengan fokus pada tiga komponen utama, yaitu pengetahuan, sikap, dan perilaku. Hasil dari penelitian ini diharapkan dapat digunakan untuk penelitian lanjutan ataupun program pengabdian masyarakat terkait edukasi keamanan siber di tingkat SMP.

1.2 Rumusan Masalah

Rumusan masalah ditetapkan di penelitian ini, sehingga penelitian tetap terfokus dan tidak melebar ke area yang tidak relevan. Terdapat dua rumusan masalah yang ditetapkan di penelitian ini, yaitu:

- a. Bagaimana tingkat kesadaran keamanan siber siswa SMP di Kabupaten Nganjuk?
- b. Bagaimana perbedaan dari tingkat kesadaran keamanan siber berdasarkan dari faktor demografis siswa?

1.3 Lingkup Penelitian

Lingkup penelitian merujuk pada batasan-batasan yang ditetapkan dalam sebuah penelitian untuk menentukan area yang akan diteliti dan fokus dari penelitian tersebut. Batasan objek penelitian ini sebagai berikut:

- a. Penelitian ini hanya mencakup dua sekolah SMP di Kabupaten Nganjuk, yaitu di SMPN 1 Ngetos dan SMP Progresif Baitul Atieq. Penelitian ini mungkin tidak mewakili tingkat kesadaran di daerah lain.
- b. Penelitian ini akan fokus pada analisis tingkat kesadaran siswa SMP mengenai keamanan siber, yang mencakup pengetahuan, sikap, dan perilaku mereka terkait dengan penggunaan teknologi informasi dan internet.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengukur tingkat kesadaran siswa SMP terhadap keamanan siber berdasarkan faktor demografis, seperti gender, kelas, asal sekolah, dan uang saku harian siswa.

1.5 Manfaat Penelitian

Harapan dari penelitian yang dilakukan adalah supaya dapat dijadikan sebagai pedoman terkait kesadaran keamanan siber pada siswa SMP di Nganjuk. Dari penelitian yang dilakukan ini juga diharapkan dapat dijadikan sumber informasi terkait tingkat kesadaran siswa SMP terhadap keamanan siber berdasarkan faktor demografis yang berbeda dari masing-masing siswa.

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Studi Literatur

Studi literatur memiliki manfaat penting dalam penelitian yang membantu membangun dasar pengetahuan yang solid dan memastikan kualitas penelitian. Dengan meninjau literatur yang ada, dapat dirumuskan pertanyaan penelitian yang lebih spesifik dan relevan, serta menghindari duplikasi dari penelitian sebelumnya. Selain itu, studi literatur memberikan wawasan tentang metodologi yang telah digunakan, membantu peneliti merancang metodologi yang lebih efektif.

b. Pengumpulan Data

Pengumpulan data dalam penelitian ini bertujuan untuk memperoleh informasi yang diperlukan untuk menganalisis kesadaran keamanan siber pada siswa SMP di Nganjuk. Data yang akan dikumpulkan mencakup data primer yang diperoleh melalui survei.

c. Analisis data

Setelah pengumpulan data, analisis data dilakukan menggunakan metode berdasarkan studi literatur yang telah dilakukan. Penelitian ini menggunakan model Kruger-Kearney untuk menganalisis data yang telah terkumpul. Hasil analisis disajikan dalam laporan yang mencakup grafik, tabel, dan rekomendasi yang didasarkan pada temuan penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan pada laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan adalah bagian yang memperkenalkan topik penelitian dan memberikan konteks serta latar belakang yang diperlukan. Pada bab ini menguraikan

latar belakang penelitian, rumusan masalah, lingkup penelitian, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II KAJIAN PUSTAKA

Pada kajian pustaka diuraikan beragam teori, konsep, dan hasil dari penelitian sebelumnya yang serupa dengan topik penelitian. Pada bagian ini menguraikan teori keamanan siber, model untuk analisis keamanan siber, dan penelitian sebelumnya yang serupa dengan topik penelitian.

BAB III METODOLOGI PENELITIAN

Bagian ini bertujuan untuk memberikan pemahaman yang jelas tentang bagaimana penelitian dilakukan dan bagaimana hasilnya diperoleh. Pada bab ini berisi populasi dan sampel pada penelitian, instrumen penelitian, dan analisis data.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas mengenai hasil dari penelitian yang telah dilakukan. Pada bab ini menguraikan demografis responden, pengukuran kesadaran keamanan siber, dan hasil dari pengukuran kesadaran keamanan siber.

BAB V KESIMPULAN DAN SARAN

Dengan menyusun kesimpulan dan saran, penelitian dapat disampaikan secara efektif dan dapat memberikan arahan yang berguna untuk tindakan lebih lanjut. Bagian ini menguraikan kesimpulan dan saran berdasarkan pengukuran kesadaran keamanan siber pada siswa SMP di Nganjuk.

BAB II

KAJIAN PUSTAKA

Pada kajian pustaka diuraikan beragam teori, konsep, dan hasil dari penelitian sebelumnya yang serupa dengan topik penelitian, sehingga dapat memberikan wawasan yang komprehensif serta mendukung metodologi penelitian. Pada bagian ini menguraikan teori keamanan siber, model untuk analisis keamanan siber, dan penelitian sebelumnya yang serupa dengan topik penelitian.

2.1 Keamanan Siber

Keamanan siber merujuk pada praktik melindungi sistem komputer, keamanan jaringan, dan keamanan data dari ancaman digital yang melibatkan peretasan, pencurian data, dan gangguan layanan (Whitman & Mattord, 2009). Menurut Stallings et al. (2015), keamanan siber melibatkan berbagai strategi dan alat yang dirancang untuk mencegah dan mendeteksi ancaman serta melindungi data dan sistem informasi.

2.1.1 Kesadaran Keamanan Siber

Kesadaran keamanan siber mencakup pemahaman tentang ancaman dan akibat dari penggunaan teknologi informasi dan komunikasi serta langkah-langkah untuk melindungi diri dari ancaman tersebut. Menurut Kruger & Kearney (2006), kesadaran keamanan siber dapat dinilai melalui pemahaman seseorang tentang ancaman seperti *malware*, *phishing*, dan *ransomware*, serta penerapan praktik keamanan yang baik. Mereka mengembangkan prototipe untuk menilai kesadaran keamanan informasi yang mencakup berbagai aspek penting seperti penggunaan kata sandi yang kuat dan pengenalan tanda-tanda *phishing*.

Shropshire et al. (2015) menyoroti pentingnya faktor kepribadian, sikap, dan niat dalam adopsi awal perilaku keamanan informasi. Mereka menemukan bahwa faktor-faktor ini berpengaruh signifikan terhadap bagaimana individu mengadopsi praktik keamanan seperti menjaga kerahasiaan data pribadi dan menggunakan jaringan yang aman. Penelitian mereka menunjukkan bahwa pendekatan holistik yang mencakup aspek psikologis dan perilaku dapat meningkatkan efektivitas program kesadaran keamanan siber.

2.1.2 Kesadaran Keamanan Siber Pada Siswa SMP

Williams & Merten (2008) menunjukkan bahwa remaja, termasuk siswa SMP sering kali kurang menyadari pentingnya privasi dan cenderung berbagi informasi pribadi secara berlebihan di media sosial. Oleh karena itu, pendekatan yang lebih holistik dalam pendidikan keamanan siber, yang mencakup aspek teknis dan sosial, sangat diperlukan untuk menciptakan lingkungan digital yang aman bagi kalangan remaja, termasuk siswa SMP.

2.1.3 Faktor-Faktor yang Memengaruhi Kesadaran Keamanan Siber

Kesadaran keamanan siber dipengaruhi oleh berbagai faktor, termasuk pengetahuan, sikap, pengalaman, dan lingkungan sosial. Penelitian sebelumnya telah mengidentifikasi beberapa faktor kunci yang berkontribusi terhadap tingkat kesadaran keamanan siber pada individu. Beberapa faktor yang memengaruhi kesadaran keamanan siber antara lain:

a. Pengetahuan dan Pendidikan

Pengetahuan merupakan faktor utama dalam kesadaran keamanan siber. Menurut Kruger & Kearney (2006), pendidikan yang memadai mengenai ancaman siber dan cara mengatasi ancaman tersebut dapat meningkatkan kesadaran keamanan siber. Mereka menyarankan penerapan program pendidikan yang mencakup informasi tentang *malware*, *phishing*, dan praktik keamanan dasar seperti penggunaan kata sandi yang kuat.

b. Sikap dan Niat

Shropshire et al. (2015) menyatakan bahwa sikap dan niat individu juga berperan penting dalam adopsi perilaku keamanan informasi. Individu yang memiliki sikap positif terhadap pentingnya keamanan siber cenderung lebih sadar dan berhati-hati dalam aktivitas *online* mereka. Faktor-faktor psikologis ini dapat ditingkatkan melalui pendekatan pendidikan yang interaktif dan berbasis pengalaman.

c. Pengalaman dan Paparan

Pengalaman dan paparan terhadap insiden keamanan siber dapat meningkatkan kesadaran individu. Menurut penelitian oleh Hadlington (2017), mereka yang pernah mengalami atau mengetahui insiden keamanan cenderung lebih waspada dan mengambil tindakan pencegahan. Oleh karena itu, simulasi insiden keamanan siber dalam berbagai setting dapat menjadi cara efektif untuk meningkatkan kesadaran.

d. Lingkungan Sosial dan Dukungan Keluarga

Lingkungan sosial, termasuk dukungan dari keluarga, teman, dan rekan kerja, juga memengaruhi kesadaran keamanan siber. Williams & Merten (2008) menunjukkan bahwa diskusi terbuka tentang keamanan siber di rumah dan tempat kerja dapat membantu individu memahami pentingnya melindungi informasi pribadi mereka. Dukungan dan contoh positif dari orang-orang yang ada di sekitar merupakan peran penting dalam membentuk sikap dan perilaku terhadap keamanan siber.

e. Teknologi dan Akses

Akses terhadap teknologi yang aman dan perangkat lunak keamanan juga berkontribusi pada kesadaran keamanan siber. Menurut penelitian oleh Livingstone et al. (2011), individu yang menggunakan perangkat dengan perlindungan keamanan yang baik cenderung lebih sadar tentang risiko yang ada dan cara melindungi diri mereka.

2.2 Metode untuk Mengukur Kesadaran Keamanan Siber

Metode pengukuran yang dapat digunakan untuk mengukur kesadaran keamanan siber bervariasi. Memahami beberapa metode diperlukan untuk menemukan metode yang sesuai dengan penelitian yang akan dilakukan. Dalam tinjauan ini, akan dipaparkan beberapa metode yang telah digunakan dalam mengukur kesadaran keamanan siber.

2.2.1 Kruger dan Kearney

Metodologi Kruger dan Kearney diterapkan sebagai alat untuk membuat alat pengukuran yang menggunakan metode yang mengadopsi dari bidang psikologi sosial. Teori psikologi sosial digunakan untuk mengukur dengan cara mendefinisikan apa yang berpengaruh atau tidak sama sekali pada objek tertentu yang mempunyai tiga komponen, di antaranya adalah pengaruh, perilaku, dan pemahaman. Kemudian Kruger-Kearney mengadopsi teori itu untuk dikembangkan berupa dimensi, yang meliputi pengetahuan, sikap, dan perilaku yang diistilahkan dengan KAB (*Knowledge, Attitude, dan Behavior*) (Kruger & Kearney, 2006).

2.2.2 *Human Aspect of Information Security Questionnaire (HAIS-Q)*

Human Aspect of Information Security Questionnaire (HAIS-Q) adalah alat evaluasi yang dikembangkan untuk mengukur kesadaran, pemahaman, dan perilaku individu terkait keamanan informasi. HAIS-Q dirancang untuk membantu organisasi menilai sejauh mana pengetahuan dan sikap karyawan mereka mengenai keamanan informasi diterjemahkan

menjadi perilaku yang aman dalam berbagai situasi. Instrumen ini mencakup beberapa dimensi utama keamanan informasi, termasuk pengelolaan kata sandi, penggunaan email, dan kesadaran terhadap ancaman sosial (Parsons et al., 2017).

2.2.3 Structural Equation Modeling (SEM)

Structural Equation Modeling (SEM) adalah teknik statistik yang menggabungkan analisis faktor dan analisis jalur untuk menguji hubungan antara variabel laten dan variabel teramati. Dalam konteks mengukur kesadaran keamanan siber, SEM memungkinkan peneliti untuk mengembangkan dan menguji model teoritis yang mencakup faktor-faktor seperti pengetahuan, sikap, dan perilaku terkait keamanan siber. Model ini dapat membantu memahami bagaimana berbagai aspek kesadaran keamanan siber berinteraksi dan mempengaruhi satu sama lain (Kline, 2018).

2.3 Kesadaran Keamanan Siber yang Harus Dipahami oleh Siswa SMP

Salvail (2020) juga menekankan pentingnya pendidikan keamanan siber di sekolah dan menyediakan sumber daya dan strategi bagi guru untuk mengajarkan konsep keamanan siber kepada siswa, sehingga dapat membantu meningkatkan kesadaran dan keterampilan mereka dalam melindungi informasi pribadi dan berperilaku aman secara *online*. Beberapa kesadaran yang harus dimiliki diantaranya adalah: privasi *online*, kesadaran *phishing*, *malware* dan virus, keamanan internet, jejak digital, dan keamanan dalam memainkan gim *online*.

2.3.1 Pengelolaan Kata Sandi

Pengelolaan kata sandi adalah proses yang bertujuan untuk memastikan keamanan dan kekuatan kata sandi yang digunakan oleh pengguna, serta menghindari kemungkinan kata sandi tersebut mudah ditebak (Grassi et al., 2017). Proses ini mencakup praktik seperti pembuatan kata sandi yang baik, penyimpanan yang baik, pengelolaan kata sandi yang baik, dan pembaruan secara berkala. Tujuan utama dari pengelolaan kata sandi adalah untuk melindungi akun dan data pribadi dari akses yang tidak sah.

2.3.2 Phishing Awareness

Kesadaran *phishing* merupakan aspek penting dalam keamanan siber yang bertujuan untuk mengedukasi individu dan organisasi tentang risiko serta tanda-tanda serangan *phishing*. *Phishing* adalah metode penipuan yang digunakan oleh pelaku kejahatan siber untuk

mendapatkan informasi pribadi, seperti nama pengguna, kata sandi, dan informasi kartu kredit dengan menyamar sebagai orang yang dapat diandalkan (Clare Stouffer, 2023).

2.3.3 Internet Safety

Keselamatan internet atau keamanan internet merujuk pada upaya dan langkah-langkah yang diambil untuk menjaga keamanan komputer, jaringan, dan data dari akses, serangan, atau kerusakan yang tidak sah. Menurut Livingstone et al. (2011), keselamatan internet mencakup perlindungan terhadap informasi pribadi, keuangan, serta keamanan komunikasi digital.

2.3.4 Online Privacy

Online privacy atau privasi daring adalah hak individu untuk mempertahankan data pribadi mereka agar tetap aman dan tidak diakses atau disalahgunakan oleh pihak ketiga tanpa izin. Dalam era digital saat ini, di mana banyak aktivitas dilakukan secara daring, menjaga privasi *online* menjadi sangat penting untuk melindungi data pribadi dari pencurian, penyalahgunaan, dan pelanggaran.

Online privacy merujuk pada hak individu untuk mengontrol informasi pribadi mereka di internet. Ini mencakup perlindungan terhadap pengumpulan, penggunaan, dan penyebaran informasi pribadi tanpa izin. Privasi daring adalah tentang menjaga data pribadi seperti identitas, riwayat penelusuran, dan komunikasi tetap aman dari akses yang tidak sah (Clare Stouffer, 2023).

2.4 Hubungan Faktor Demografis Terhadap Kesadaran Keamanan Siber

Kajian ini bertujuan untuk mengeksplorasi hubungan antara berbagai faktor demografis dan kesadaran keamanan siber. Dengan memahami bagaimana faktor-faktor ini saling berhubungan, dihasilkan hasil pengukuran keamanan siber yang efektif.

2.4.1 Kesadaran Keamanan Siber Berdasarkan Gender

Menurut Ramadhani dan Pratama (2020), terdapat perbedaan signifikan dalam tingkat kesadaran keamanan siber antara pria dan wanita. Pria cenderung memiliki tingkat kesadaran yang lebih tinggi terkait dengan risiko dan praktik keamanan siber dibandingkan wanita. Hal ini mungkin disebabkan oleh perbedaan dalam keterlibatan teknologi dan paparan terhadap informasi keamanan.

2.4.2 Kesadaran Keamanan Siber Berdasarkan Kelas

Tingkat pendidikan, termasuk tingkatan kelas pada sekolah dan pengalaman dengan teknologi berperan penting dalam menentukan kesadaran keamanan siber. Individu dengan pendidikan yang lebih tinggi dan pengalaman lebih banyak dalam menggunakan teknologi umumnya memiliki kesadaran yang lebih baik mengenai praktik keamanan siber (Ramadhani & Pratama, 2020).

2.4.3 Kesadaran Keamanan Siber Berdasarkan Asal Sekolah

Ramadhani dan Pratama (2020) menemukan bahwa semakin tinggi intensitas penggunaan media sosial, semakin besar pula risiko pengguna terpapar ancaman keamanan siber. Hal ini terutama terjadi jika pengguna tidak memiliki kesadaran yang cukup tentang praktik keamanan yang aman saat menggunakan media sosial. Berdasarkan hasil survei di SMPN 1 Ngetos dan SMP Progresif Baitul Atieq, siswa dari SMPN 1 Ngetos lebih sering menggunakan sosial media daripada siswa dari SMP Progresif Baitul Atieq. Hal ini menjadikan menarik untuk melakukan pengukuran kesadaran keamanan siber berdasarkan asal sekolah.

2.4.4 Kesadaran Keamanan Siber Berdasarkan Uang Saku Harian

Berdasarkan hasil survei di SMPN 1 Ngetos dan SMP Progresif Baitul Atieq, siswa yang memiliki uang saku dengan jumlah besar lebih sering mengakses sosial media daripada siswa dengan uang saku sedikit. Hal ini menjadikan menarik untuk melakukan pengukuran kesadaran keamanan siber berdasarkan jumlah uang saku harian siswa.

2.5 Tinjauan Pustaka

Dalam penelitian ini, dibahas tiga studi sebelumnya yang mirip dengan masalah yang diteliti mengenai “Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk“. Didapatkan hasil penelitian sebagai berikut:

- a. Dalam penelitian yang telah dilakukan oleh Kusumaningrum et al. (2022) dengan judul "Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat *Study from Home* dengan *Multiple Criteria Decision Analysis (MCDA)*" yang dipublikasikan di Jurnal Ilmiah SINUS 20.1 (2022): 69-78 menghasilkan temuan:
 1. Pengetahuan tentang Ancaman Siber: Banyak mahasiswa memiliki pengetahuan dasar tentang ancaman siber tetapi kurang memahami detail teknis dan implikasi dari ancaman tersebut.

2. Penggunaan *Password* dan Keamanan Data: Terdapat kelemahan dalam praktik penggunaan *password* yang kuat dan perlindungan data pribadi. Mahasiswa seringkali menggunakan *password* yang mudah ditebak atau sama untuk beberapa akun.
 3. Praktik Keamanan *Online*: Mahasiswa menunjukkan kesadaran yang rendah terhadap pentingnya menjaga privasi online dan kewaspadaan terhadap penipuan *online*.
- b. Penelitian oleh Ramadhani & Pratama (2020) mengeksplorasi nilai kesadaran keamanan siber pada pengguna media sosial di Indonesia. Mereka menemukan bahwa tingkat skor keamanan siber di antara pengguna media sosial di Indonesia masih perlu ditingkatkan (Ramadhani & Pratama, 2020). Dari penelitian yang dilakukan juga menekankan bahwa edukasi dan kampanye kesadaran penting untuk meningkatkan pemahaman dan perilaku aman dalam menggunakan media sosial (Ramadhani & Pratama, 2020). Temuan tersebut relevan bagi upaya untuk meningkatkan kesadaran keamanan siber di berbagai kelompok pengguna internet, termasuk siswa SMP.
- c. Penelitian oleh Nurdin & Rahman (2023) mengukur tingkat kesadaran keamanan siber di kalangan mahasiswa Teknik Informatika di Universitas Widyatama. Mereka menemukan bahwa "meskipun sebagian besar mahasiswa memiliki pengetahuan dasar tentang keamanan siber, banyak dari mereka yang tidak secara konsisten menerapkan praktik keamanan yang baik" (Nurdin & Rahman, 2023). Penelitian ini juga menekankan bahwa "perlunya program pelatihan yang lebih intensif dan berkelanjutan untuk meningkatkan kesadaran dan keterampilan keamanan siber di kalangan mahasiswa" (Nurdin & Rahman, 2023). Temuan ini memberikan wawasan penting bagi upaya peningkatan kesadaran keamanan siber di berbagai kelompok pendidikan, termasuk siswa SMP.

Penelitian ini berbeda dengan penelitian sebelumnya yang hanya fokus pada kalangan mahasiswa dan pengguna media sosial di Indonesia. Penelitian yang mengkaji kesadaran keamanan siber yang fokus pada siswa SMP masih jarang ditemukan. Terlebih lagi, belum ada penelitian yang meneliti kesadaran keamanan siber di kalangan santri pondok pesantren yang sehari-hari jarang menggunakan gawai. Meskipun demikian, santri pondok pesantren tetap

berisiko menjadi korban kejahatan siber karena mereka sesekali menggunakan gawai untuk berkomunikasi dengan orang di luar pondok pesantren.

BAB III

METODOLOGI PENELITIAN

Metode kuantitatif diterapkan pada penelitian ini, yang didasarkan pada filsafat *positivisme*. *Positivisme* adalah cara untuk mendekati kebenaran melalui metode ilmiah, berfokus pada fakta-fakta dan bukti-bukti yang dapat diobservasi (Aswani, 2015). Metode pengambilan sampel biasanya diambil secara acak. Data dikumpulkan ke dalam suatu instrumen penelitian, yang kemudian analisis dari data kuantitatif atau data statistik. Tujuan utamanya adalah untuk menguji hipotesis yang telah ditetapkan (Sugiyono, 2013).

Metode Kruger dan Kearney dipilih untuk mengukur kesadaran keamanan siber pada siswa SMP di Nganjuk karena pendekatan ini menawarkan kerangka evaluasi yang komprehensif dan telah terbukti efektif dalam berbagai penelitian. Metode ini tidak hanya menilai pengetahuan dasar tentang keamanan siber, tetapi juga mencakup sikap dan perilaku siswa terkait dengan ancaman keamanan siber, memberikan gambaran yang menyeluruh tentang tingkat kesadaran mereka (Kruger & Kearney, 2006). Aspek-aspek yang diukur, seperti kesadaran terhadap phishing, penggunaan kata sandi yang aman, dan privasi digital, sangat relevan dengan tantangan yang dihadapi oleh siswa SMP saat ini, sehingga membuat metode ini cocok digunakan dalam konteks pendidikan menengah.

3.1 Populasi

Populasi merujuk pada seluruh wilayah yang terdiri dari objek ataupun subjek dengan mutu dan penggunaan ketentuan yang telah diatur oleh peneliti, sehingga dapat ditelaah dan diambil kesimpulannya (Sugiyono, 2013). Populasi tidak terbatas pada manusia saja, tetapi bisa berupa objek dan benda alam lainnya. Populasi tidak hanya mencakup berapa objek atau subjek yang diteliti, tetapi juga semua karakter dan ciri-ciri dari objek ataupun subjek tersebut. Pada penelitian ini, populasi yang akan digunakan adalah siswa SMP di Nganjuk, baik dari sekolah negeri maupun swasta, yang terdiri dari kelas VII, VIII, dan IX. Berdasarkan informasi dari situs web Dinas Pendidikan Kabupaten Nganjuk (2023), jumlah siswa SMP negeri di Nganjuk sebanyak 30.155 siswa, sementara jumlah siswa SMP swasta di Nganjuk sejumlah 4.984 siswa.

3.2 Sampel

Sampel adalah bagian dari populasi yang memiliki karakteristik tertentu yang diteliti (Sugiyono, 2013). Ketika jangkauan populasi sangat besar dan tidak mungkin untuk meneliti

seluruh anggotanya, yang disebabkan karena kurangnya tenaga, dana, dan waktu, peneliti bisa memakai sampel pada populasi tersebut. Sampel yang sudah ditentukan ini kemudian diterapkan pada keseluruhan populasi. Oleh karena itu, penggunaan sampel yang digunakan harus bersifat representatif. Dalam penerapannya, Sugiyono (2019) memberikan contoh penggunaan metode Slovin dalam berbagai penelitian survei, terutama ketika peneliti harus bekerja dengan populasi besar dan tidak memiliki informasi rinci tentang variabilitas populasi tersebut.

Metode Slovin merupakan salah satu metode yang sering digunakan dalam penelitian untuk menentukan ukuran sampel dari populasi besar. Sugiyono (2019) menjelaskan bahwa metode ini sangat berguna dalam penelitian kuantitatif, terutama dalam konteks survei, di mana peneliti perlu memastikan bahwa sampel yang diambil cukup representatif dengan tingkat kesalahan tertentu. Rumus Slovin membantu peneliti menghitung ukuran sampel yang optimal, menghindari pengambilan sampel yang terlalu besar atau terlalu kecil, yang dapat mempengaruhi validitas hasil penelitian. Setelah dilakukan sampling dari jumlah populasi siswa SMP negeri dan swasta di Nganjuk dengan total 35.139 siswa, didapatkan sampling sejumlah 99,7, yang kemudian dibulatkan menjadi 100 siswa dengan tingkat kesalahan (*margin of error*) sebesar 10%.

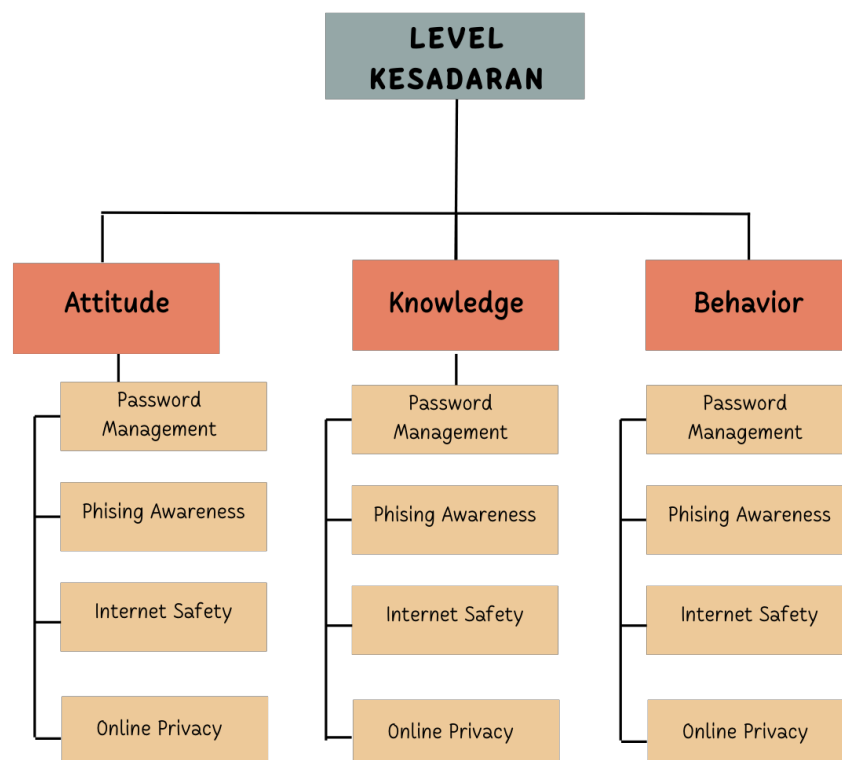
Jumlah sampel pada penelitian ini sedikit lebih kecil dari jumlah sampling yang telah dilakukan. Penelitian ini menggunakan sampel sejumlah 99 siswa, yang terdiri dari 49 siswa SMPN 1 Ngetos (mewakili SMP negeri) dan 50 siswa SMP Progresif Baitul Atieq (mewakili SMP swasta berbasis pondok pesantren). Sampel dari SMPN 1 Ngetos terdiri dari 15 siswa kelas VII, 13 siswa kelas VIII, dan 21 siswa kelas IX. Dari SMP Progresif Baitul Atieq, terdapat sampel yang terdiri dari 15 siswa kelas VII, 19 siswa kelas VIII, dan 16 siswa kelas IX.

3.3 Instrumen Penelitian

Kuesioner yang dibuat pada penelitian ini, dibuat dalam bentuk Google Form untuk siswa SMPN 1 Ngetos, yang diperbolehkan membawa gawai, serta lembar kuesioner untuk sekolah SMP swasta berbasis pondok pesantren yang tidak diperbolehkan membawa gawai. Hasil kuesioner dikumpulkan dalam Google Sheet untuk mempermudah analisis data. Responden akan menjawab kuesioner sesuai dengan pengetahuan atau pengalaman mereka. Pertanyaan dalam kuesioner dikembangkan berdasarkan model Kruger-Kearney, yang diadaptasi dari teori

psikologi sosial dan membagi pengukuran objek menjadi tiga komponen: *cognition* (kognisi), *affection* (afeksi), dan *behavior* (perilaku).

Ketiga komponen tersebut kemudian diadopsi untuk dikembangkan dengan jumlah dimensi yang sama yang dinamakan *knowledge*, *attitude*, dan *behavior* (Kruger & Kearney, 2006). Terdapat topik yang berjumlah empat pada penelitian ini, yaitu *password management* (kesadaran siswa terhadap penggunaan *password*), *phishing awareness* (kesadaran siswa terhadap ancaman *phishing*), *internet safety* (kesadaran siswa menggunakan internet dengan aman), dan *online privacy* (kesadaran siswa untuk menjaga privasi di internet). Dari keempat tersebut memiliki dimensi masing-masing berupa pertanyaan. Keempat topik tersebut ditentukan berdasarkan artikel dari Common Sense Media dengan judul “*Teacher’s Essential Guide to Cybersecurity*”, yang menjelaskan beberapa kesadaran keamanan siber yang harus dipahami siswa menengah, termasuk siswa SMP (Salvail, 2020). Dari artikel ini didapatkan empat topik kesadaran keamanan siber yang harus dipahami siswa SMP. Kerangka kesadaran pada penelitian ini ditampilkan pada Gambar 3.1.



Gambar 3.1 Kerangka pengukur kesadaran keamanan siber

Pada topik *password management* berisi pertanyaan terkait bagaimana siswa SMP mengelola dan menyimpan kata sandi secara aman untuk berbagai akun dan layanan *online*. Topik *phishing awareness* berisi pertanyaan apa yang dilakukan untuk mengenali dan menghindari serangan *phishing*. Pada topik *internet safety*, berisi pertanyaan langkah-langkah yang diambil untuk melindungi diri dan data pribadi saat menggunakan internet. Terakhir, pada topik *online privacy* berisi pertanyaan cara yang benar untuk melindungi individu dari risiko penyalahgunaan informasi, seperti pencurian identitas, pelanggaran data, dan pengawasan yang tidak diinginkan.

Dengan menyesuaikan pilihan kata pada setiap kalimat pada setiap topik dalam setiap dimensi, lalu ditentukanlah kuesioner untuk mengetahui kesadaran keamanan siber pada siswa SMP di Nganjuk, seperti yang ditunjukkan dalam Gambar 3.2.

Contoh pertanyaan untuk uji Knowledge:

Saya boleh memakai *password* yang sama antara *password* akun media sosial dan selain media sosial (Contoh: akun email, belanja *online*, akun game).

1. Sangat Setuju
2. Setuju
3. Netral
4. Tidak Setuju
5. Sangat tidak Setuju

Contoh pertanyaan untuk uji Attitude:

Menurut saya, aman-aman saja memakai *password* yang sama antara *password* media sosial dengan akun selain media sosial (Contoh: akun email, belanja *online*, akun game).

1. Sangat Setuju
2. Setuju
3. Netral
4. Tidak Setuju
5. Sangat tidak Setuju

Contoh pertanyaan untuk uji Behavior:

Saya memakai *password* yang tidak sama untuk akun media sosial dengan akun selain media sosial (Contoh: akun email, belanja online, akun game).

1. Sangat Setuju
2. Setuju
3. Netral
4. Tidak Setuju
5. Sangat tidak Setuju

Gambar 3.2 Gambaran daftar kuesioner

Mengacu pada Model Kruger & Kearney, gambaran kuesioner pada penelitian ini telah dirancang sesuai dengan dimensi dan topik yang diteliti, yaitu kesadaran keamanan siber. Dari setiap dimensi *knowledge*, *attitude* dan *behavior*, diberikan lima opsi jawaban, yaitu sangat setuju, setuju, netral, tidak setuju, dan sangat tidak setuju.

3.4 Analisis Data

Kuesioner dalam penelitian yang dilakukan terbagi atas dua kelompok, yaitu kuesioner berdasarkan demografis dan kuesioner yang berguna untuk menghitung skor tingkat kesadaran. Bagian survei demografis terdiri dari informasi tentang gender, kelas, asal sekolah, dan uang saku harian. Bagian yang digunakan untuk menghitung skor tingkat kesadaran terdiri dari 36 soal yang dirancang untuk menilai kesadaran keamanan siber siswa SMP. Kuesioner ini dibuat oleh peneliti dengan masukan dari dosen pembimbing, yang kemudian diteliti berdasarkan metode Kruger-Kearney. Metode ini mengadopsi dari teori psikologi sosial, yang membagi pengukuran objek menjadi tiga komponen: *cognition* (kognisi), *affection* (afeksi), dan *behavior* (perilaku). Ketiga komponen ini kemudian diadaptasi menjadi tiga dimensi, yaitu *Knowledge*, *Attitude*, dan *Behavior* (Kruger & Kearney, 2006). Semua 36 soal yang disusun mengadopsi pertanyaan dari HAIS-Q (*The Human Aspects of Information Security Questionnaire*) items (Parsons et al., 2017). Pertanyaan tersebut disesuaikan berdasarkan empat topik yang diperoleh dari Common Sense Media dengan judul “*Teacher’s Essential Guide to Cybersecurity* yang kemudian akan dianalisis menggunakan metode Kruger dan Kearney. Pada tiap dimensi KAB, terdapat pernyataan untuk tiap topik kesadaran keamanan siber: pernyataan 1—3 tentang pengelolaan *password*, 4—6 tentang *phishing awareness*, 7—9 tentang *internet safety*, dan 10—12 tentang *online privacy*. Kuesioner tersusun dari pernyataan positif dan negatif untuk memastikan responden teliti untuk membaca setiap pertanyaan. Pernyataan positif diberi nilai dalam rentang 4—0, sementara pernyataan negatif diberi nilai dalam rentang 0—4. Pada Tabel 3.1 dipaparkan daftar pertanyaan yang diajukan ke responden.

Tabel 3.1 Daftar Pertanyaan

Dimensi	Pertanyaan	Pilihan Jawaban
<i>Knowledge</i>	1. Saya boleh menggunakan <i>password</i> yang sama antara <i>password</i> akun media sosial dan selain media sosial (Contoh: akun email, belanja <i>online</i> , akun game).*	• Sangat Setuju

	<ol style="list-style-type: none"> 2. Saya boleh membagikan <i>password</i> saya kepada teman saya.* 3. Saya harus mengkombinasikan huruf besar, huruf kecil, angka, dan karakter khusus saat membuat <i>password</i>. 4. Saya boleh klik tautan di Whatsapp dari pengirim yang dikenal.* 5. Saya tidak diperbolehkan klik tautan di Whatsapp dari pengirim yang tidak dikenali. 6. Saya boleh membuka file pada pesan dari pengirim pesan yang tidak dikenali.* 7. Saya boleh mengunduh file apapun dari internet.* 8. Saat saya belajar di sekolah, saya dilarang mengakses situs web tertentu. 9. Saya boleh membagikan semua informasi di semua situs web jika diminta.* 10. Saya harus mengecek pengaturan privasi pada akun media sosial secara berkala. 11. Menurut saya, tidak ada sanksi karena sesuatu yang saya bagikan di media sosial.* 12. Saya boleh mengeposkan apa saja yang saya inginkan pada media sosial.* 	<ul style="list-style-type: none"> • Setuju • Netral • Tidak Setuju • Sangat Tidak Setuju
<i>Attitude</i>	<ol style="list-style-type: none"> 1. Menurut saya, aman-aman saja menggunakan password yang sama antara password media sosial dengan akun selain media sosial (Contoh: akun email, belanja <i>online</i>, akun game).* 2. Membagikan password kepada teman adalah hal buruk, meskipun dengan teman dekat saya. 3. Aman saja menggunakan <i>password</i> yang terdiri dari hanya kombinasi huruf saja.* 4. Mengklik tautan di Whatsapp dari pengirim yang dikenal selalu aman.* 5. Tidak ada dampak buruk yang akan terjadi ketika saya mengklik tautan di Whatsapp dari pengirim yang tidak dikenali.* 6. Ada risikonya ketika membuka lampiran pada pesan dari pengirim yang tidak dikenal. 7. Mengunduh file dari internet memiliki risiko. 8. Hanya dikarenakan saya diperbolehkan membuka situs tertentu di sekolah, bukan berarti situs tersebut aman. 9. Bila perlu, tidak masalah memasukkan informasi apapun di semua situs web.* 10. Ide bagus untuk meninjau privasi pada akun sosial media secara berkala. 11. Tidak masalah ketika saya mengeposkan hal-hal pada media sosial yang biasanya tidak saya ucapkan di depan umum.* 12. Ada risikonya ketika mengeposkan apa saja yang saya mau pada media sosial. 	<ul style="list-style-type: none"> • Sangat Setuju • Setuju • Netral • Tidak Setuju • Sangat Tidak Setuju
	<ol style="list-style-type: none"> 1. Saya memakai <i>password</i> yang berbeda pada akun media sosial dengan selain media sosial (Contoh: akun email, belanja <i>online</i>, akun game). 	<ul style="list-style-type: none"> • Sangat Setuju

<p><i>Behavior</i></p>	<ol style="list-style-type: none"> 2. Saya memberikan <i>password</i> yang saya miliki kepada teman dekat saya.* 3. Saya menggunakan kombinasi huruf kecil, huruf besar, angka, dan karakter khusus untuk semua <i>password</i>. 4. Saya tidak selalu mengklik tautan di Whatsapp hanya karena tautan tersebut berasal dari orang yang saya kenali. 5. Jika pesan dari pengirim yang tidak saya dikenal terlihat menarik, saya akan mengklik tautannya.* 6. Saya tidak membuka file pada pesan jika pengirimnya tidak saya kenal. 7. Saya mengunduh file apapun jika file tersebut saya butuhkan.* 8. Ketika saya mengakses internet di sekolah, saya mengunjungi situs web apa saja yang saya butuhkan.* 9. Saya memastikan keamanan situs web sebelum memasukkan informasi tentang saya di internet 10. Saya tidak meninjau privasi di akun media sosial secara berkala.* 11. Saya tidak mengupload apapun di media sosial sebelum mempertimbangkan dampak negatifnya 12. Saya membagikan apapun yang saya mau di media sosial.* 	<ul style="list-style-type: none"> • Setuju • Netral • Tidak Setuju • Sangat Tidak Setuju
------------------------	---	---

Catatan: Pernyataan yang diberi tanda bintang(*) merupakan pernyataan negatif.

Penelitian ini menggunakan jenis data primer, yang diperoleh langsung dari siswa SMPN 1 Ngetos dan siswa SMP Progresif Baitul Atieq. Data primer dikumpulkan melalui survei atau kuesioner yang dirancang menggunakan Google Form untuk SMPN 1 Ngetos dan lembar kuesioner untuk SMP Progresif Baitul Atieq. Kuesioner merupakan cara pengambilan data, yang dilakukan dengan cara memberikan beberapa pertanyaan tulis untuk responden yang kemudian dijawabnya (Sugiyono, 2013). Pendistribusian kuesioner ini diajukan kepada responden dengan cara: (1) Mengunjungi SMPN 1 Ngetos untuk meminta izin kepada Kepala Sekolah dengan membawa surat permohonan pengisian kuesioner untuk kesediaannya mengizinkan muridnya agar dapat mengisi kuesioner. Setelah diberi izin, peneliti membagikan kepada OSIS berupa *link* Google Form pengisian kuesioner. (2) Mengunjungi SMP Progresif Baitul Atieq yang berbasis Pondok Pesantren dengan membawa surat permohonan pengisian kuesioner untuk meminta izin kepada Kepala Sekolah untuk kesediaannya mengizinkan muridnya agar dapat mengisi kuesioner. Setelah diberi izin, peneliti membagikan kepada OSIS berupa Lembar angket pengisian kuesioner.

Dalam penelitian ini, kuesioner berlangsung dengan menghabiskan waktu dua minggu, yaitu dari tanggal 18 Maret 2024 sampai 31 Maret 2024. Kuesioner berhasil mendapatkan data dari 29 responden di SMP Negeri dan 50 responden di SMP Swasta. Data dari kuesioner Google Form di-*generate* ke dalam Google Sheet, untuk data kuesioner yang berupa lembar angket dimasukkan ke dalam Google Form oleh peneliti sehingga data terkumpul menjadi satu di Google Sheet.

Penelitian ini menganalisis data secara kuantitatif. Nilai responden dari setiap pertanyaan ditentukan berdasarkan ketentuan dari penilaian yang sudah ditetapkan, sesuai dengan jawaban yang mereka pilih secara jujur. Penilaian ini mencakup pengetahuan responden tentang kesadaran keamanan siber, sikap responden, dan kebiasaan responden dalam sehari-hari. Pertama, penghitungan skor dilakukan untuk masing-masing jawaban dari responden. Setiap pilihan jawaban yang mereka pilih memiliki skor yang berbeda. Penilaian dari kuesioner ini dapat dilihat pada Tabel 3.2.

Tabel 3.2 Penilaian dari Kuesioner

Soal bersifat Positif	Soal bersifat Negatif
Sangat Setuju : 4	Sangat Setuju : 0
Setuju : 3	Setuju : 1
Netral : 2	Netral : 2
Tidak Setuju : 1	Tidak Setuju : 3
Sangat Tidak Setuju : 0	Sangat Tidak Setuju : 4

Pembobotan pada penelitian ini dilakukan di setiap dimensi, yang diperoleh melalui konsultasi bersama dosen pembimbing sebagai manajer penelitian. Persentase pembobotan pada setiap dimensi dihitung berdasarkan kontribusi masing-masing dimensi terhadap kesadaran siswa SMP. Dimensi *behavior* diberikan bobot tertinggi karena dianggap memberi kontribusi yang paling banyak terhadap kesadaran keamanan siber. Pada dimensi *knowledge* dan *attitude* memiliki bobot yang lebih rendah. Bobot setiap dimensi yang diterapkan untuk menghitung skor kesadaran dan pembagian pertanyaan untuk setiap topik, terdapat dalam Tabel 3.3 dan Tabel 3.4.

Tabel 3.3 Pembobotan Dimensi

Dimensi	Bobot
----------------	--------------

<i>Knowledge</i>	30%
<i>Attitude</i>	20%
<i>Behavior</i>	50%

Tabel 3.4 Pembagian Pertanyaan untuk Setiap Topik

Topik	Pertanyaan
<i>Password Management</i>	1,2,3
<i>Phishing Awareness</i>	4,5,6
<i>Internet Safety</i>	7,8,9
<i>Online Privacy</i>	10,11,12

Selanjutnya, dilakukan pengukuran tingkat kesadaran dilakukan berdasarkan hasil survei yang diperoleh. Hasil dari penghitungan ini akan mengungkapkan tingkat kesadaran keamanan siber pada responden, baik secara menyeluruh, individual, atau berdasarkan kategori demografis dari hasil survei. Model Kruger-Kearney membolehkan penyesuaian skala kesadaran seperti skala yang sudah tersedia (Kruger & Kearney, 2006). Penentuan skala kesadaran pada penelitian ini diatur melalui konsultasi bersama dosen pembimbing, yang berperan sebagai manajer penelitian. Tingkat kesadaran diukur berdasarkan skala kesadaran yang tercantum dalam Tabel 3.5, yang diadaptasi dari model Kruger-Kearney dan diadaptasikan hanya pada penelitian ini.

Tabel 3.4 Skala Kesadaran

Kriteria	Nilai (%)
<i>Baik</i>	80 - 100
<i>Sedang</i>	60 - 79
<i>Buruk</i>	0 - 59

BAB IV

HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas mengenai hasil dari penelitian yang telah dilakukan. Hasil penelitian akan disajikan dalam bentuk tabel, grafik, dan deskripsi naratif yang mendetail.

4.1 Demografis Responden

Tabel 4.1 menyajikan data demografis 99 responden yang terkumpul dalam penelitian ini. Semua responden dikelompokkan dalam berbagai kategori, termasuk gender, kelas, sekolah negeri/swasta, dan uang saku harian.

Tabel 4.1 Demografis responden

Demografis	Jumlah	Persentase
Gender		
Laki-laki	42	42,4%
Perempuan	57	57,6%
Kelas		
VII	30	30,3%
VIII	32	32,3%
IX	37	37,4%
Asal Sekolah		
SMPN 1 Ngetos	49	49,5%
SMP Progresif Baitul Atieq	50	50,5%
Uang saku per hari		
< Rp5000,00	16	16,2 %
Rp5000,00 – Rp10.000,00	71	71,7 %
> Rp10.000,00	12	12,1 %

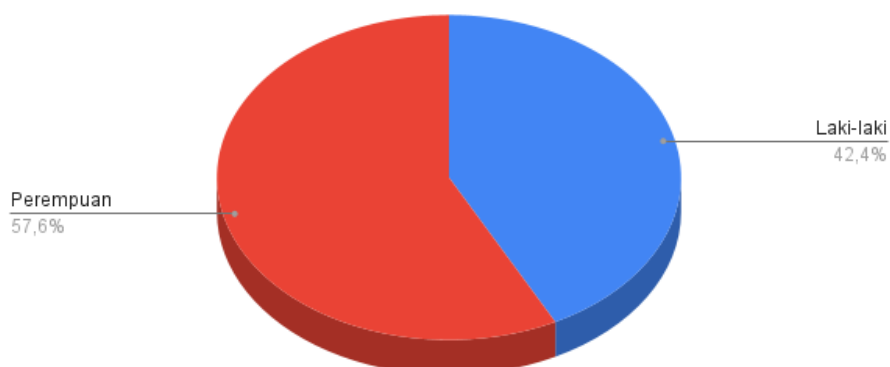
Dari seluruh responden yang mengisi kuesioner, terdapat lebih banyak perempuan dibandingkan laki-laki, walaupun selisihnya hanya sedikit. Sebanyak 57 responden adalah perempuan, sementara 42 responden adalah laki-laki, dengan selisih sebesar 15 responden. Sejumlah 57,6% dari seluruh responden adalah perempuan, sementara 42,4% adalah laki-laki. Lalu dari segi kelas, persebarannya cukup seimbang, dengan 30,3% responden berasal dari kelas

7, 32,3% responden berasal dari kelas VIII, dan 37,4% berasal dari kelas IX. Lebih jelasnya, 30 responden didapatkan dari kelas VII, 32 responden didapatkan dari kelas VIII, dan 37 responden didapatkan dari kelas IX. Kemudian dari segi asal sekolah, jumlahnya hanya selisih satu. Siswa dari SMPN 1 Ngetos terdapat 49 siswa dengan persentase dari keseluruhan, yaitu 49,5%. Sementara itu, jumlah siswa dari SMP Progresif Baitul Atieq adalah 50 siswa dengan persentase 50,5%. Selanjutnya, dari segi uang saku, terdapat perbedaan yang sangat signifikan. Sebanyak 71 responden dalam kuesioner penelitian ini memiliki uang saku antara Rp5.000,00 hingga Rp10.000,00, yang merupakan 71,7% dari total responden. Sementara itu, terdapat 16 siswa atau 16,2% dari seluruh responden dengan uang saku kurang dari Rp5000,00. Selanjutnya, 12 siswa atau 12,1% dari seluruh jumlah responden dengan uang saku lebih dari Rp10.000,00.

4.1.1 Persentase Responden Berdasarkan Gender

Persentase gender responden dapat dilihat pada Gambar 4.1 :

Berdasarkan Gender



Gambar 4.1 Persentase responden berdasarkan gender

Dari Gambar 4.1, dapat diketahui bahwa siswa terbanyak di penelitian ini adalah perempuan, dengan jumlah 57 orang atau 57,6% dari total responden. Sementara itu, terdapat 42 responden laki-laki, yang mewakili 42,4% dari total responden.

4.1.2 Persentase Jumlah Responden Berdasarkan Kelas

Gambar 4.2 menunjukkan persentase responden berdasarkan kelas.



Gambar 4.2 Jumlah responden berdasarkan kelas

Gambar 4.2 menunjukkan persentase distribusi responden berdasarkan kelas, yaitu VII, VIII, atau IX. Dari segi kelas, jumlah responden di ketiga kelas tidak terlalu berbeda dan cenderung seimbang. Secara rinci, 30,3% responden berasal dari kelas VII, 32,3% berasal dari kelas VIII, dan 37,4% berasal dari kelas IX. Dengan jumlah yang lebih spesifik, terdapat 30 responden dari kelas VII, 32 responden dari kelas VIII, dan 37 responden dari kelas IX.

4.1.3 Persentase Responden Berdasarkan Asal Sekolah

Persentase jumlah responden berdasarkan asal sekolah dapat dilihat pada Gambar 4.3.

Jumlah responden berdasarkan asal sekolah



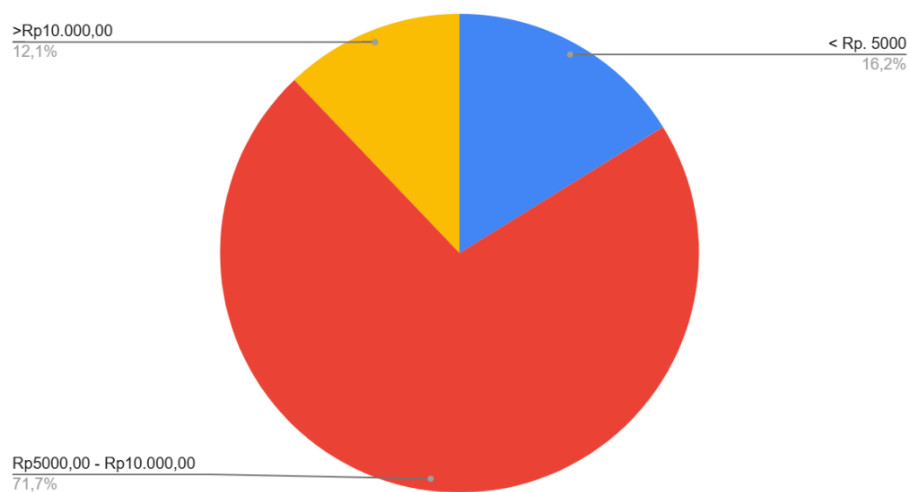
Gambar 4.3 Jumlah responden berdasarkan asal sekolah

Berdasarkan asal sekolah, jumlahnya hanya selisih satu. Siswa dari SMPN 1 Ngetos terdapat 49 siswa dengan persentase dari keseluruhan, yaitu 49,5%. Sementara itu, jumlah siswa dari SMP Progresif Baitul Atieq adalah 50 siswa dengan persentase 50,5%.

4.1.4 Persentase Responden Berdasarkan Uang Saku

Persentase uang saku responden dapat dilihat dari Gambar 4.4.

Jumlah responden berdasarkan uang saku



Gambar 4.4 Persentase uang saku responden

Berdasarkan pada Gambar 4.3, sebagian besar responden kuesioner penelitian ini memiliki uang saku antara Rp5000,00 – Rp10.000,00 setiap harinya terdapat 71 Responden atau 71,7% dari keseluruhan responden. Sementara 16 siswa atau 16,2% dari seluruh responden dengan uang saku kurang dari Rp5000,00. Selanjutnya, 12 siswa atau 12,1% dari seluruh jumlah responden dengan uang saku lebih dari Rp10.000,00.

4.2 Analisis Skor Kesadaran

Setelah mengetahui demografis responden, dilakukan pengukuran kesadaran keamanan siber dari nilai setiap pertanyaan. Pengukuran skor kesadaran diukur menggunakan model Kruger-Kearney, dengan masing-masing nilai berkaitan dengan dimensi dan topik yang berbeda. Hasil pengukuran ini akan menunjukkan nilai akhir yang mencerminkan tingkat kesadaran keamanan siber secara keseluruhan. Dari hasil pengukuran, disajikan gambar hasil pengukuran yang mencakup nilai kesadaran keamanan pada setiap topik dan dimensi, total kesadaran per dimensi, total kesadaran per topik, dan skor kesadaran total. Nilai kesadaran yang berada pada level buruk ditandai dengan warna merah. Lalu, nilai kesadaran yang berada pada level sedang ditandai dengan warna kuning. Nilai kesadaran yang berada di level baik ditandai dengan warna hijau. Untuk nilai kesadaran yang dilingkari, menunjukkan angka kesadaran total.

Berikut merupakan proses menghitung dari nilai setiap pertanyaan agar didapatkan nilai kesadaran berdasarkan metode Kruger-Kearney:

1. Masing-masing nilai dari hasil kuesioner pada Google Form dan lembar kuesioner dari responden dimasukkan ke Google Sheet, yang disajikan pada Gambar 4.5

The screenshot shows an Excel spreadsheet with a formula bar containing: `=IF('Form Responses 1'!N2 = 5; 0; IF('Form Responses 1'!N2 = 4; 1; IF('Form Responses 1'!N2 = 3; 2; IF('Form Responses 1'!N2 = 2; 3; IF('Form Responses 1'!N2 = 1; 4; ""))))`

F	G	H	I	J	K	L	M	N
a.k1 (Negatif)	a.k2 (Negatif)	a.k3 (Positif)	a.a1 (negatif)	a.a2 (Positif)	a.a3 (negatif)	a.b1 (Positif)	a.b2 (negatif)	a.b3 (Positif)
2	1	3	3	2	3	1	1	1
3	4	1	3	3	2	2	4	2
1	4	2	3	4	2	4	4	2
2	3	3	1	3	2	3	1	2
4	4	3	3	3	1	3	3	3
2	4	0	2	0	2	2	3	0
3	3	2	2	3	2	3	0	2
2	2	3	3	1	3	3	1	0
2	3	2	2	2	4	0	2	0
4	4	1	3	0	3	3	4	2
4	4	2	3	0	3	1	4	2
2	4	2	4	2	4	2	4	2
4	4	0	4	0	4	0	4	0
4	3	1	4	1	4	2	3	1
3	4	2	3	3	2	2	4	2
1	2	3	2	1	1	2	1	3
4	4	2	3	2	1	3	2	2
1	3	3	1	3	1	1	3	1
2	4	2	2	0	2	2	4	2
2	2	2	2	3	2	2	2	2
3	3	1	3	1	1	1	3	1
1	3	3	2	3	0	3	2	3
1	1	4	1	1	2	3	1	2
3	3	1	3	3	1	3	1	3
3	1	2	1	3	1	4	2	3

Gambar 4.7 Pengolahan pertanyaan negatif

3. Nilai responden pada setiap topik dan dimensi, dimasukkan ke sheet yang baru seperti pada Gambar 4.8.

Password Management Knowledge		
Penilaian		
2	1	3
3	4	1
1	4	2
2	3	3
4	4	3
2	4	0
3	3	2
2	2	3
2	3	2
4	4	1
4	4	2
2	4	2
4	4	0
4	3	1
3	4	2
1	2	3
4	4	2
1	3	3
2	4	2
2	2	2
3	3	1
1	3	3
1	1	4
3	3	1

Gambar 4.8 Topik setiap dimensi masing-masing responden

4. Nilai dari masing-masing responden dijumlahkan agar menghasilkan nilai total pertanyaan (NTP) seperti Gambar 4.9.

Password Management Knowledge			
Penilaian			Nilai Total
2	1	3	6
3	4	1	8
1	4	2	7
2	3	3	8
4	4	3	11
2	4	0	6
3	3	2	8
2	2	3	7
2	3	2	7
4	4	1	9
4	4	2	10
2	4	2	8
4	4	0	8
4	3	1	8
3	4	2	9
1	2	3	6
4	4	2	10
1	3	3	7
2	4	2	8
2	2	2	6
3	3	1	7
1	3	3	7
1	1	4	6
3	3	1	7

Gambar 4.9 Nilai total pertanyaan (NTP)

5. Hasil dari NTP dirata-rata melalui persamaan (4.1), lalu dihasilkan seperti pada Gambar 4.10.

$$\text{rata - rata NTP} = \frac{\text{NTP}}{\text{Jumlah Pertanyaan per topik}} \quad (4.1)$$

Password Management Knowledge				NTP= Nilai Total
Penilaian			Nilai Total	Rata-rata NTP
2	1	3	6	2
3	4	1	8	2,666666667
1	4	2	7	2,333333333
2	3	3	8	2,666666667
4	4	3	11	3,666666667
2	4	0	6	2
3	3	2	8	2,666666667
2	2	3	7	2,333333333
2	3	2	7	2,333333333
4	4	1	9	3
4	4	2	10	3,333333333
2	4	2	8	2,666666667
4	4	0	8	2,666666667
4	3	1	8	2,666666667
3	4	2	9	3
1	2	3	6	2
4	4	2	10	3,333333333
1	3	3	7	2,333333333
2	4	2	8	2,666666667
2	2	2	6	2
3	3	1	7	2,333333333
1	3	3	7	2,333333333
1	1	4	6	2
3	3	1	7	2,333333333

Gambar 4.10 Penghitungan rata-rata NTP

6. Nilai rata-rata NTP tersebut kemudian dibagi dengan 4 (Poin tertinggi skala likert), untuk mendapatkan nilai variabel Z setiap responden seperti pada Gambar 4.11.

Password Management Knowledge				NTP= Nilai Total	Pertanyaan
Penilaian			Nilai Total	Rata-rata NTP	NTP/4 (Z)
2	1	3	6	2	0,5
3	4	1	8	2,666666667	0,666666667
1	4	2	7	2,333333333	0,583333333
2	3	3	8	2,666666667	0,666666667
4	4	3	11	3,666666667	0,916666667
2	4	0	6	2	0,5
3	3	2	8	2,666666667	0,666666667
2	2	3	7	2,333333333	0,583333333
2	3	2	7	2,333333333	0,583333333
4	4	1	9	3	0,75
4	4	2	10	3,333333333	0,833333333
2	4	2	8	2,666666667	0,666666667
4	4	0	8	2,666666667	0,666666667
4	3	1	8	2,666666667	0,666666667
3	4	2	9	3	0,75
1	2	3	6	2	0,5
4	4	2	10	3,333333333	0,833333333
1	3	3	7	2,333333333	0,583333333
2	4	2	8	2,666666667	0,666666667
2	2	2	6	2	0,5
3	3	1	7	2,333333333	0,583333333
1	3	3	7	2,333333333	0,583333333
1	1	4	6	2	0,5
3	3	1	7	2,333333333	0,583333333

Gambar 4.11 Skor variabel Z masing-masing responden

7. Seluruh nilai dari variabel Z kemudian dijumlahkan seperti Gambar 4.12.

fx =SUM(J3:J101)

Password Management Knowledge				NTP= Nilai Total	Pertanyaan	
Penilaian			Nilai Total	Rata-rata NTP	NTP/4 (Z)	sum (Z)
2	1	3	6	2	0,5	66,08333333
3	4	1	8	2,666666667	0,666666667	
1	4	2	7	2,333333333	0,583333333	
2	3	3	8	2,666666667	0,666666667	
4	4	3	11	3,666666667	0,916666667	
2	4	0	6	2	0,5	
3	3	2	8	2,666666667	0,666666667	
2	2	3	7	2,333333333	0,583333333	
2	3	2	7	2,333333333	0,583333333	
4	4	1	9	3	0,75	
4	4	2	10	3,333333333	0,833333333	
2	4	2	8	2,666666667	0,666666667	
4	4	0	8	2,666666667	0,666666667	
4	3	1	8	2,666666667	0,666666667	
3	4	2	9	3	0,75	
1	2	3	6	2	0,5	
4	4	2	10	3,333333333	0,833333333	
1	3	3	7	2,333333333	0,583333333	
2	4	2	8	2,666666667	0,666666667	
2	2	2	6	2	0,5	
3	3	1	7	2,333333333	0,583333333	
1	3	3	7	2,333333333	0,583333333	
1	1	4	6	2	0,5	
3	3	1	7	2,333333333	0,583333333	

Gambar 4.12 Penjumlahan variabel Z

8. Skor kesadaran setiap topik dan dimensi didapatkan dengan melakukan pembagian dari nilai Sum(Z) dengan banyak responden keseluruhan, dengan menggunakan persamaan (4.2). Setelah itu, nilai kesadaran diubah menjadi bentuk persentase seperti Gambar 4.13.

$$Skor\ kesadaran = \frac{Sum(Z)}{Jumlah\ Responden} \quad (4.2)$$

Password Management Knowledge				NTP= Nilai Total Pertanyaan		
Penilaian	Nilai Total	Rata-rata NTP	NTP/4 (Z)	sum (Z)	Skor	
2	1	3	6	2	0,5	
3	4	1	8	2,666666667	0,666666667	
1	4	2	7	2,333333333	0,583333333	
2	3	3	8	2,666666667	0,666666667	
4	4	3	11	3,666666667	0,916666667	
2	4	0	6	2	0,5	
3	3	2	8	2,666666667	0,666666667	
2	2	3	7	2,333333333	0,583333333	
2	3	2	7	2,333333333	0,583333333	
4	4	1	9	3	0,75	
4	4	2	10	3,333333333	0,833333333	
2	4	2	8	2,666666667	0,666666667	
4	4	0	8	2,666666667	0,666666667	
4	3	1	8	2,666666667	0,666666667	
3	4	2	9	3	0,75	
1	2	3	6	2	0,5	
4	4	2	10	3,333333333	0,833333333	
1	3	3	7	2,333333333	0,583333333	
2	4	2	8	2,666666667	0,666666667	
2	2	2	6	2	0,5	
3	3	1	7	2,333333333	0,583333333	
1	3	3	7	2,333333333	0,583333333	
1	1	4	6	2	0,5	
3	3	1	7	2,333333333	0,583333333	

Gambar 4.13 Skor kesadaran setiap topik dan dimensi

9. Nilai kesadaran setiap topik dan dimensi kemudian ditempatkan ke dalam tabel kesadaran berdasarkan dengan topik dan dimensinya seperti Gambar 4.14.

Topik	total kesadaran per dimensi			
Password Management				66,75%
Phishing Awareness				
Internet Safety				
Online Privacy				
	Behavior (50)	Attitude (20)	Knowledge (30)	total kesadaran per topik

Gambar 4.14 Input skor berdasarkan masing-masing topik dan masing-masing dimensi

10. Dengan penghitungan yang sama, kemudian diterapkan dengan semua topik lain, sehingga seluruh nilai kesadaran lengkap seperti Gambar 4.15.

Topik	total kesadaran per dimensi			
Password Management	63,47%	58,08%	66,75%	
Phishing Awareness	58,84%	62,63%	58,16%	
Internet Safety	55,56%	60,10%	55,56%	
Online Privacy	61,70%	65,32%	61,70%	
	Behavior (50)	Attitude (20)	Knowledge (30)	total kesadaran per topik

Gambar 4.15 Input skor semua topik

11. Total kesadaran per dimensi (TD) dihitung rata-ratanya, dengan menggunakan persamaan (4.3).

$$TD = \frac{\text{Total kesadaran per dimensi}}{4} \quad (4.3)$$

A	B	C	D	E	F	G	I
Topik		total kesad:	59,89%	61,53%	60,54%		
	Password Management		63,47%	58,08%	66,75%		
	Phishing Awareness		58,84%	62,63%	58,16%		
	Internet Safety		55,56%	60,10%	55,56%		
	Online Privacy		61,70%	65,32%	61,70%		
			Behavior (50)	Attitude (20)	Knowledge (30)		total kesadaran per topik

Gambar 4.16 penghitungan kesadaran per dimensi (TD)

12. Total kesadaran per topik (TP) dihitung rata-ratanya, dengan menggunakan persamaan (4.4) seperti pada Gambar 4.17.

$$TP = \frac{\text{Nilai kesadaran per topik}}{3} \quad (4.4)$$

A	B	C	D	E	F	G
Topik		total kesad:	59,89%	61,53%	60,54%	
	Password Management		63,47%	58,08%	66,75%	62,77%
	Phishing Awareness		58,84%	62,63%	58,16%	59,88%
	Internet Safety		55,56%	60,10%	55,56%	57,07%
	Online Privacy		61,70%	65,32%	61,70%	62,91%
			Behavior (50)	Attitude (20)	Knowledge (30)	total kesadaran per topik

Gambar 4.17 Nilai kesadaran per topik

13. Nilai rata-rata total kesadaran per dimensi dan rata-rata total kesadaran per topik dihitung seperti Gambar 4.18 dengan persamaan (4.5) dan persamaan (4.6).

$$\text{Rata - rata TD} = \frac{\text{Total TD}}{3} \quad (4.5)$$

$$\text{Rata-rata TP} = \frac{\text{Total TP}}{4} \quad (4.6)$$

D	E	F	G	H	I	J
59,89%	61,53%	60,54%			Rata-rata kesada	60,66%
63,47%	58,08%	66,75%	62,77%		Rata-rata kesada	60,66%
58,84%	62,63%	58,16%	59,88%			
55,56%	60,10%	55,56%	57,07%			
61,70%	65,32%	61,70%	62,91%			
Behavior (50)	Attitude (20)	Knowledge (30)	total kesadaran per topik			

Gambar 4.18 Rata-rata kesadaran TD dan TP

14. Terakhir, untuk skor kesadaran akhir, dihitung seperti Gambar 4.19 dengan menggunakan persamaan (4.7).

$$\text{Skor Kesadaran Akhir} = \frac{((TD \text{ Behavior} * 0,5) + (TD \text{ Attitude} * 0,2) + (TD \text{ Knowledge} * 0,3) + \text{ratarata TD})}{2} \quad (4.7)$$

A	B	C	D	E	F	G	H
Topik		total kesada	59,89%	61,53%	60,54%	60,53%	
Password Management			63,47%	58,08%	66,75%	62,77%	
Phishing Awareness			58,84%	62,63%	58,16%	59,88%	
Internet Safety			55,56%	60,10%	55,56%	57,07%	
Online Privacy			61,70%	65,32%	61,70%	62,91%	
			Behavior (50)	Attitude (20)	Knowledge (30)	total kesadaran per topik	

Gambar 4.19 Hasil akhir skor kesadaran

15. Pada pengukuran berdasarkan demografis, menggunakan cara yang sama, yaitu dengan menghitung berdasarkan masing-masing demografisnya.

4.2.1 Nilai Kesadaran Keseluruhan Responden

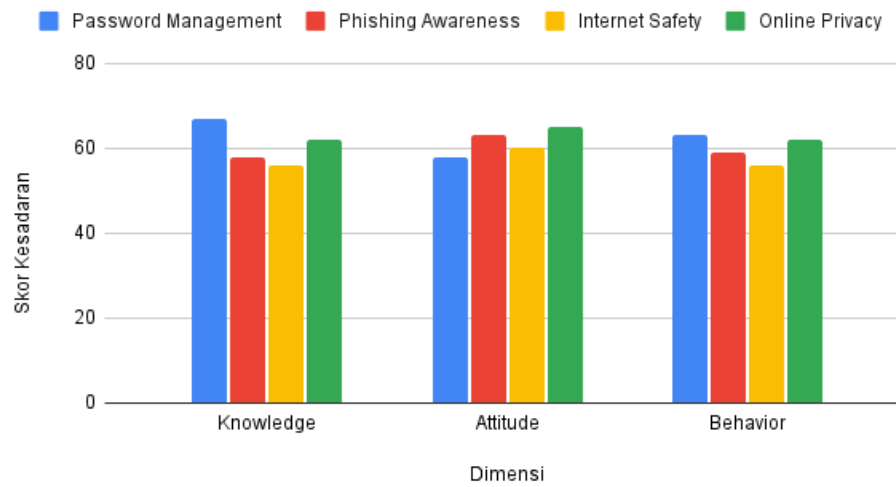
Total kesadaran per dimensi	60	62	61	61
Password management	63	58	67	63
Phishing awareness	59	63	58	60
Internet Safety	56	60	56	57
Online Privacy	62	65	62	63
	Behavior (50)	Attitude (20)	Knowledge (30)	Total Kesadaran Per topik

Gambar 4.20 Nilai kesadaran keseluruhan responden

Hasil pengukuran kesadaran keamanan siber yang diperoleh setelah melakukan analisis terhadap keseluruhan responden dapat dilihat pada Gambar 4.20. Berdasarkan Gambar 4.20, nilai kesadaran keamanan siber pada siswa SMP di Nganjuk berada di angka 61, yang termasuk level sedang dan mendekati tingkat buruk. Artinya, kesadaran keamanan siber pada siswa SMP di Nganjuk masih perlu ditingkatkan.

Dimensi *attitude* mendapatkan nilai tertinggi dengan nilai 62, sementara dimensi *knowledge* mendapatkan nilai 61, dan *behavior* memiliki nilai 60. Pada topik *online privacy* dan *password management*, kesadaran keamanan siber bernilai sama, yaitu di angka 63. Untuk topik *phishing awareness*, nilai kesadarannya berada di angka 60. Kesadaran terendah dan berada di level buruk terdapat pada topik *internet safety*, yaitu dengan nilai 57. Grafik skor kesadaran keseluruhan setiap topik dan dimensi terdapat pada Gambar 4.21.

Skor Kesadaran Keamanan Siber Keseluruhan



Gambar 4.21. Grafik skor kesadaran keamanan siber keseluruhan

4.2.2 Nilai Kesadaran Berdasarkan Gender

Total Kesadaran per Dimensi	58	59	59	59
<i>Password Management</i>	65	61	66	66
<i>Phishing Awareness</i>	52	60	57	56
<i>Internet Safety</i>	55	56	53	55
<i>Online Privacy</i>	59	60	61	60
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

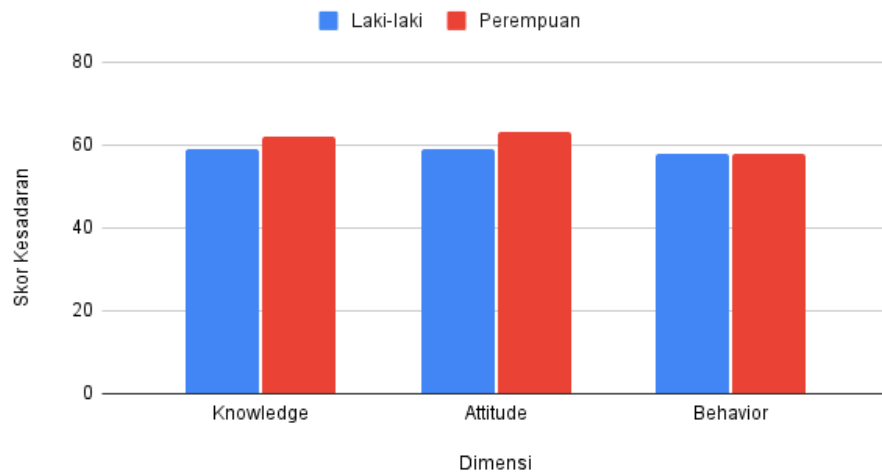
Gambar 4.22 Nilai kesadaran Laki-laki

Total Kesadaran per Dimensi	58	63	62	61
<i>Password Management</i>	63	56	67	62
<i>Phishing Awareness</i>	64	65	59	63
<i>Internet Safety</i>	53	63	57	58
<i>Online Privacy</i>	52	69	63	61
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

Gambar 4.23 Nilai kesadaran Perempuan

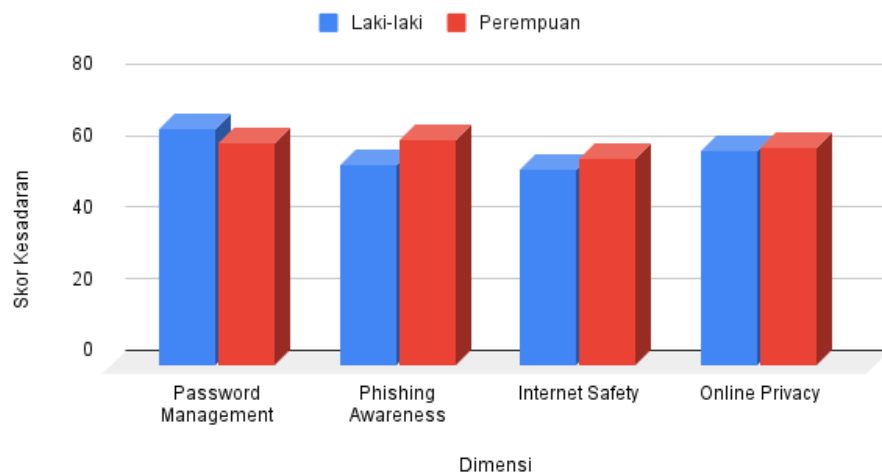
Gambar 4.22 dan Gambar 4.23 menunjukkan skor kesadaran berdasarkan gender. Tingkat kesadaran laki-laki lebih rendah dibandingkan dengan perempuan. Laki-laki memperoleh nilai kesadaran sebesar 59 persen, sedangkan perempuan mencapai skor 61 persen. Meskipun laki-laki memiliki skor kesadaran keseluruhan yang lebih rendah daripada perempuan, mereka memiliki skor kesadaran yang lebih tinggi pada topik password management, yaitu 66 persen, dibandingkan dengan perempuan yang mendapatkan skor 62 persen pada topik yang sama. Skor kesadaran dari laki-laki dan perempuan masih perlu untuk ditingkatkan karena berada pada level sedang. Perbandingan dari segi dimensi dan topik berdasarkan gender dapat dilihat pada Gambar 4.24 dan 4.25.

Perbandingan skor dimensi berdasarkan gender



Gambar 4.24 Perbandingan skor kesadaran setiap dimensi berdasarkan gender

Perbandingan skor setiap topik berdasarkan gender



Gambar 4.25 Perbandingan skor kesadaran setiap topik berdasarkan gender

4.2.3 Nilai Kesadaran Berdasarkan Kelas

Total Kesadaran per Dimensi	57	58	58	57
<i>Password Management</i>	58	55	64	59
<i>Phishing Awareness</i>	58	57	51	55
<i>Internet Safety</i>	53	56	56	55
<i>Online Privacy</i>	58	62	61	60
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

Gambar 4.26 Skor kesadaran kelas VII

Total Kesadaran per Dimensi	64	66	64	65
<i>Password Management</i>	70	62	69	67
<i>Phishing Awareness</i>	62	66	62	63
<i>Internet Safety</i>	58	66	59	61
<i>Online Privacy</i>	68	70	66	68
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

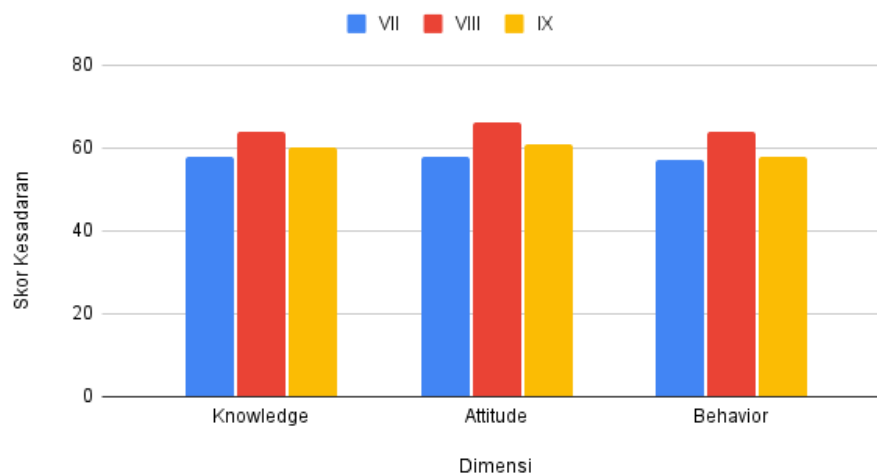
Gambar 4.27 Skor kesadaran kelas VIII

Total Kesadaran per Dimensi	58	61	60	59
<i>Password Management</i>	62	57	67	62
<i>Phishing Awareness</i>	57	64	61	61
<i>Internet Safety</i>	51	59	52	54
<i>Online Privacy</i>	62	64	59	62
	Behavior(50)	Attitude(20)	Knowledge(30)	Total Kesadaran per Topik

Gambar 4.28 Skor Kesadaran kelas IX

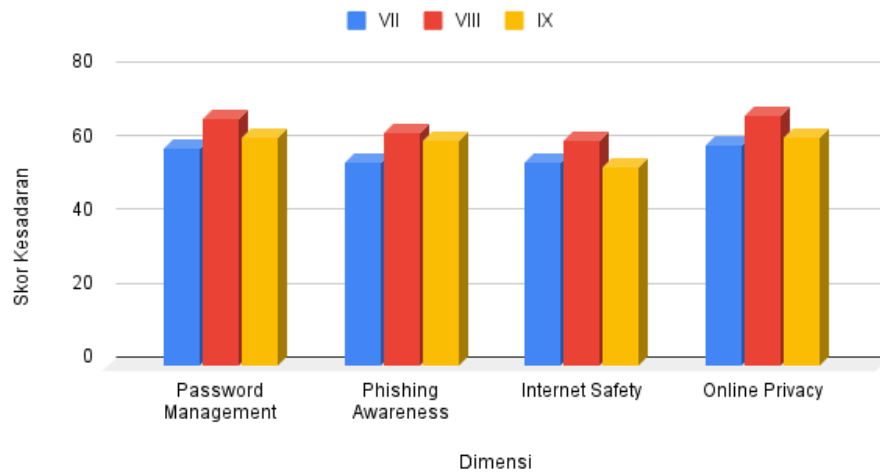
Gambar 4.26, 4.27, dan 4.28 menunjukkan perbedaan kesadaran keamanan siber berdasarkan tingkatan kelas. Skor keadaran siswa kelas VIII berada di angka paling tinggi dibandingkan kelas lain yaitu di angka 65 persen. Sementara kelas VII mendapatkan skor kesadaran 57 persen. Untuk skor kesadaran kelas IX berada di 59 persen. Dari keseluruhan skor yang didapatkan dari analisis menunjukkan bahwa kelas VIII dan IX berada pada level sedang, sementara kelas VII berada pada level buruk. Perbandingan nilai kesadaran setiap dimensi dan topik berdasarkan kelas terdapat pada gambar 4.29 dan 4.30.

Perbandingan skor setiap dimensi berdasarkan kelas



Gambar 4.29 Perbandingan nilai kesadaran setiap dimensi berdasarkan kelas

Perbandingan skor setiap topik berdasarkan kelas



Gambar 4.30 Perbandingan skor kesadaran setiap topik berdasarkan kelas

4.2.4 Nilai Kesadaran Berdasarkan Asal Sekolah

Total kesadaran per dimensi	62	65	63	63
Password management	64	62	69	65
Phishing awareness	62	69	62	64
Internet Safety	56	63	59	59
Online Privacy	65	67	62	65
	Behavior (50)	Attitude (20)	Knowledge (30)	Total Kesadaran Per topik

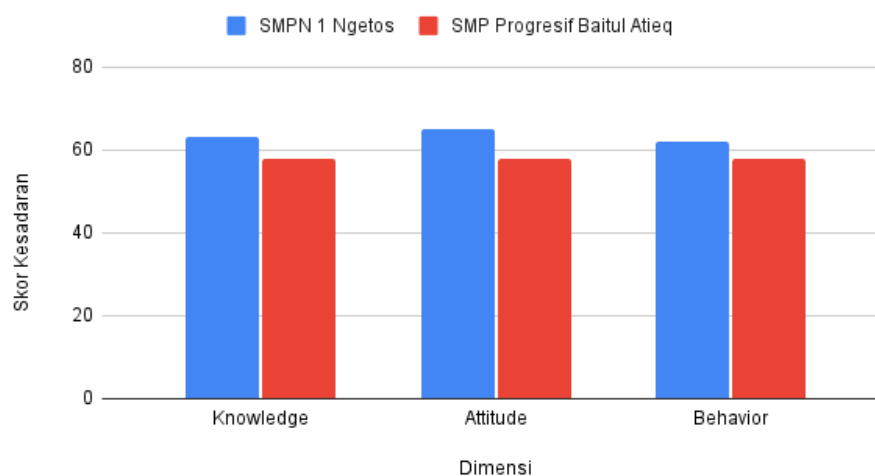
Gambar 4.31 Skor siswa SMPN 1 Ngetos

Total kesadaran per dimensi	58	58	58	58
Password management	63	54	64	60
Phishing awareness	56	56	55	55
Internet Safety	52	58	53	54
Online Privacy	60	64	61	62
	Behavior (50)	Attitude (20)	Knowledge (30)	Total Kesadaran Per topik

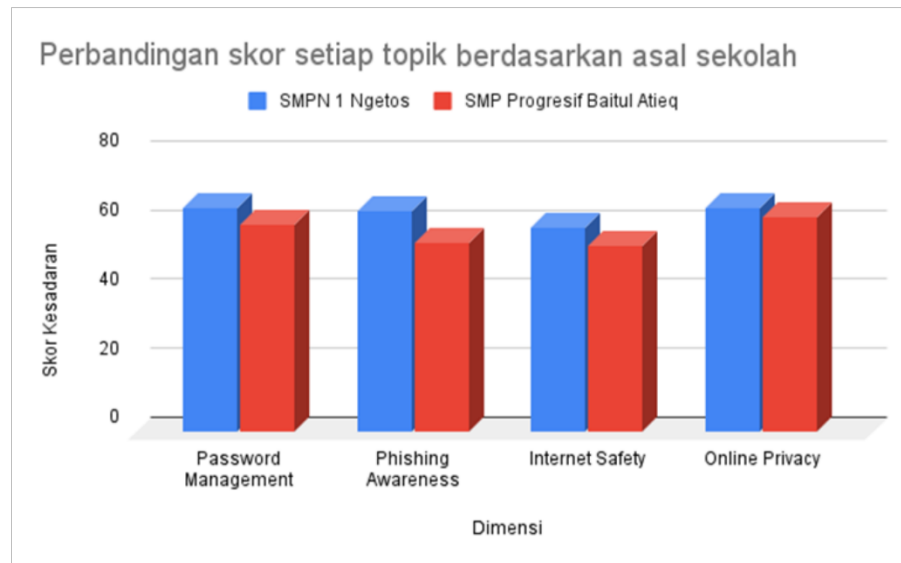
Gambar 4.32 Skor siswa SMP Progresif Baitul Atieq

Gambar 4.31 dan gambar 4.32 menunjukkan Hasil perbandingan pengukuran kesadaran keamanan siber antarsekolah menunjukkan bahwa skor kesadaran siswa SMP negeri lebih tinggi dibandingkan dengan skor kesadaran siswa sekolah SMP swasta berbasis pondok. Skor kesadaran siswa SMP negeri berada di nilai 63, sementara skor siswa SMP swasta bernilai 58. Pada topik *online privacy*, skor kesadaran siswa SMP swasta berada pada level sedang. Perbandingan skor kesadaran setiap dimensi dan topik terdapat pada Gambar 4.33 dan 4.34.

Perbandingan skor setiap dimensi berdasarkan asal sekolah



Gambar 4.33 Perbandingan skor kesadaran setiap dimensi berdasarkan asal sekolah



Gambar 4.34 Perbandingan skor kesadaran setiap topik berdasarkan asal sekolah

4.2.5 Nilai Kesadaran Berdasarkan Uang Saku

Total Kesadaran per Dimensi	56	59	60	58
<i>Password Management</i>	54	58	66	59
<i>Phishing Awareness</i>	57	66	55	59
<i>Internet Safety</i>	56	58	59	58
<i>Online Privacy</i>	56	55	60	57
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

Gambar 4.35 Skor kesadaran siswa dengan uang saku kurang dari Rp5000,00

Total Kesadaran per Dimensi	59	60	60	59
<i>Password Management</i>	65	58	66	63
<i>Phishing Awareness</i>	58	62	57	59
<i>Internet Safety</i>	54	60	55	56
<i>Online Privacy</i>	59	60	61	60
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

Gambar 4.36 Skor kesadaran siswa dengan uang saku Rp5000,00 sampai Rp10.000,00

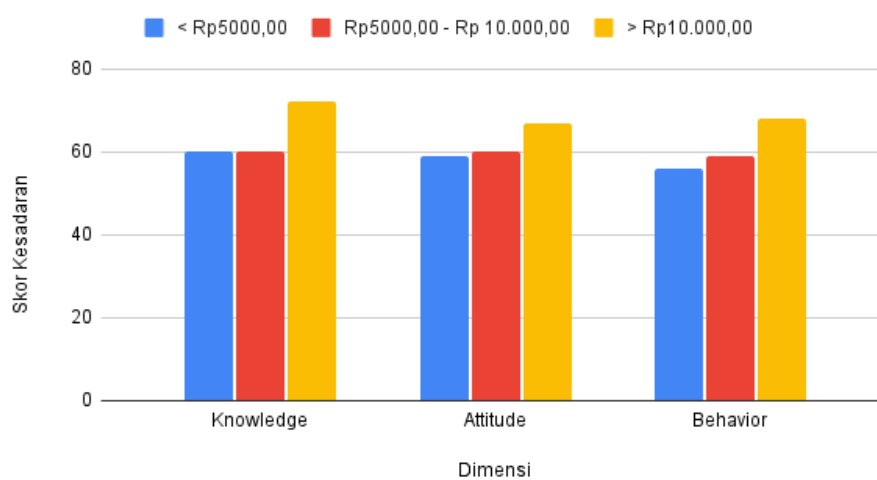
Total Kesadaran per Dimensi	68	67	72	69
<i>Password Management</i>	73	62	80	72
<i>Phishing Awareness</i>	72	68	73	71
<i>Internet Safety</i>	58	70	61	63
<i>Online Privacy</i>	70	67	73	70
	<i>Behavior(50)</i>	<i>Attitude(20)</i>	<i>Knowledge(30)</i>	Total Kesadaran per Topik

Gambar 4.37 Skor kesadaran siswa dengan uang saku lebih dari Rp10.000,00

Gambar 4.35, 4.36, dan 4.37 membagi tabel berdasarkan faktor uang saku siswa. Pada siswa uang saku lebih dari Rp10.000,00 mendapatkan skor tertinggi dan berada pada level sedang, yaitu di angka 69 persen. Sementara Skor Kesadaran Siswa dengan Uang Saku Rp5000,00 sampai Rp10.000,00 di angka 59 persen, lalu skor kesadaran siswa dengan uang saku kurang dari Rp5000,00 berada di angka 58 persen.

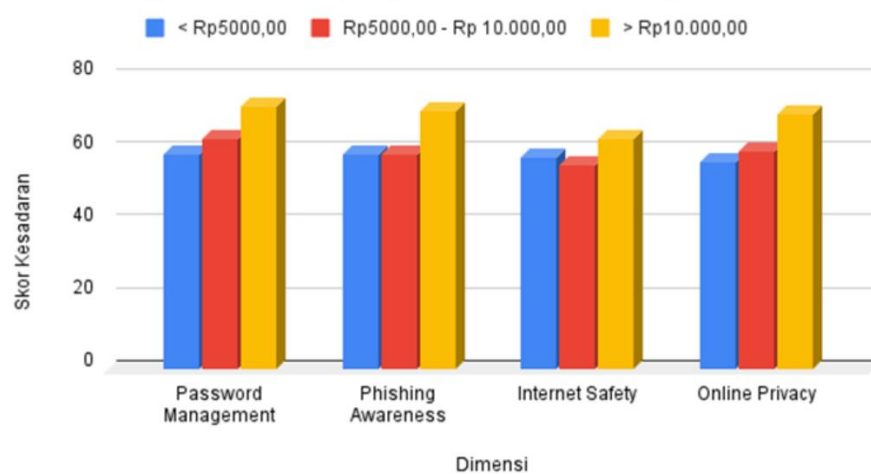
Pada dimensi *knowledge* topik *password management*, siswa dengan uang saku lebih dari Rp10.000,00 memiliki angka kesadaran pada level baik, yaitu berada di angka 80 persen. Dari perbandingan ini dapat disimpulkan bahwa jumlah uang saku juga memengaruhi tingkat kesadaran keamanan siber pada siswa SMP. Perbandingan skor kesadaran setiap dimensi dan setiap topik terdapat pada Gambar 4.38 dan 4.39.

Perbandingan skor setiap dimensi berdasarkan uang saku



Gambar 4.38 Perbandingan skor kesadaran setiap dimensi berdasarkan uang saku per hari

Perbandingan skor setiap topik berdasarkan uang saku



Gambar 4.39 Perbandingan skor kesadaran setiap topik berdasarkan uang saku per hari

4.3 Skor Kesadaran Keseluruhan dalam Bentuk Tabel

Skor kesadaran keseluruhan dari siswa SMPN 1 Ngetos dan SMP Progresif Baitul Atieq disajikan dalam bentuk tabel yang tersedia pada Tabel 4.2.

Tabel 4.2 Skor Kesadaran Keseluruhan

Faktor Demografis	Skor Kesadaran
Keseluruhan	61 %
Berdasarkan Gender	
Laki-laki	59%
Perempuan	61%
Berdasarkan Kelas	
Kelas VII	57 %
Kelas VIII	65%
Kelas IX	59%
Berdasarkan Asal Sekolah	
SMPN 1 Ngetos	63%
SMP Progresif Baitul Atieq	58%
Berdasarkan Uang Saku	
Kurang dari Rp5000,00	58%
Rp5000,00 – Rp10.000,00	59%
Lebih dari Rp10.000,00	69%

Dari hasil pengukuran kesadaran keamanan siber pada siswa SMPN 1 Ngetos dan SMP Progresif Baitul Atieq, terdapat perbedaan skor kesadaran pada setiap faktor demografis siswa. Berdasarkan gender, siswa dengan gender laki-laki memiliki skor kesadaran yang lebih rendah daripada siswa dengan gender perempuan. Berdasarkan demografis kelas, siswa kelas VIII memiliki skor kesadaran yang lebih tinggi daripada kelas VII dan IX. Meskipun tingkatan kelas IX berada di atas kelas VIII, siswa kelas IX memiliki skor kesadaran di bawah siswa kelas VIII.

Berdasarkan demografis asal sekolah, skor kesadaran siswa dari SMPN 1 Ngetos lebih tinggi daripada siswa SMP Progresif Baitul Atieq. Hal ini menunjukkan bahwa siswa dari SMP swasta berbasis pesantren yang jarang menggunakan gawai memiliki skor kesadaran lebih

rendah dibandingkan dengan siswa yang sering menggunakan gawai, seperti siswa SMP negeri. Berdasarkan demografis uang saku harian siswa, siswa dengan uang saku lebih dari Rp10.000,00 memiliki nilai kesadaran yang lebih baik daripada siswa dengan uang saku dibawah Rp10.000,00.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Secara keseluruhan, level kesadaran keamanan siber siswa SMP di Nganjuk sudah berada di level sedang, dengan total skor keseluruhan 61. Namun, skor ini mendekati level buruk. Hal ini menunjukkan bahwa edukasi keamanan siber pada siswa SMP di Nganjuk perlu diperhatikan dan ditingkatkan lagi. Edukasi kesadaran keamanan siber di kalangan siswa SMP dapat dilakukan melalui pembelajaran di sekolah dan pelatihan keamanan siber di berbagai platform yang tersedia.

Perbedaan faktor demografis juga menghasilkan nilai kesadaran yang berbeda pada setiap dimensi dan topik yang digunakan untuk pengukuran tingkat kesadaran. Dari hasil penelitian, siswa dari SMP swasta berbasis pesantren yang jarang menggunakan gawai memiliki skor kesadaran lebih rendah dibandingkan dengan siswa yang sering menggunakan gawai, seperti siswa SMP negeri.

5.2 Saran

Masih ada sebagian kekurangan dalam penelitian ini, seperti perlunya peningkatan baik dari segi kualitas maupun kuantitas pertanyaan yang diajukan untuk mengukur nilai kesadaran keamanan siber. Selain itu, demografis responden cenderung homogen, dengan sebagian besar responden berasal dari daerah yang sama, yaitu Kabupaten Nganjuk. Untuk penelitian berikutnya disarankan agar melakukan penelitian pada lingkup yang lebih luas lagi. Penelitian selanjutnya dapat dilakukan di Kabupaten yang lain, atau di tingkat Provinsi/Nasional.

DAFTAR PUSTAKA

- Aswani, D. R. (2015). Review of Richard Dawkins' The God Delusion. *Thought and Practice*, 6(1), 81. <https://doi.org/10.4314/tp.v6i1.7>
- Clare Stouffer. (2023). *What is phishing? How to spot and avoid it*. Us.Norton.Com. <https://us.norton.com/blog/online-scams/what-is-phishing>
- Dinas Pendidikan Kabupaten Nganjuk. (2023). *Jumlah Siswa PAUD, SD, SMP, Pendidikan Kesetaraan Berdasarkan Status (Negeri atau Swasta) Tahun 2023*. <https://dashboard.nganjukkab.go.id/menudataset/detail?data=ZGY4NGI0YjctYWFiZi00ZjYwLTkwNDctMTI2ZGY0MDMzZTUy>
- Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: authentication and lifecycle management*. <https://doi.org/10.6028/NIST.SP.800-63b>
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between [3 _ T D \$ D I F F] Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3, e00346. <https://doi.org/10.1016/j.heliyon.2017>
- Kline, R. B. (2018). Response to Leslie Hayduk's review of principles and practice of structural equation modeling, 1 4th edition. *Canadian Studies in Population*, 45(3–4), 188–195. <https://doi.org/10.25336/csp29418>
- Krejcie, R. V. (1970). *DETERMINING SAMPLE SIZE FOR RESEARCH ACTIVITIES* (Vol. 30).
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289–296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, 20(1), 69. <https://doi.org/10.30646/sinus.v20i1.586>
- Laurie Salvail. (2020). *Teachers' Essential Guide to Cybersecurity*. Common Sense Education. <https://www.common sense.org/education/articles/teachers-essential-guide-to-cybersecurity>

- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries Report Original citation.*
- Nuridin, H. R., & Rahman, A. A. (2023). PENGUKURAN TINGKAT KESADARAN KEAMANAN SIBER PADA PENGGUNA MEDIA SOSIAL DI LINGKUNGAN MAHASISWA TEKNIK INFORMATIKA UNIVERSITAS WIDYATAMA. *Jurnal Darma Agung*, 31(3), 94. <https://doi.org/10.46930/ojsuda.v31i3.3374>
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
- Ramadhani, M. R., & Raf'ie Pratama, A. (2020). *Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia.*
- Reza Pahlevi. (2022, June 10). *Penetrasi Internet di Kalangan Remaja Tertinggi di Indonesia.* Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). <https://databoks.katadata.co.id/datapublish/2022/06/10/penetrasi-internet-di-kalangan-remaja-tertinggi-di-indonesia>
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, 49, 177–191. <https://doi.org/10.1016/j.cose.2015.01.002>
- Stallings, W., Brown, L., Columbus, B., New, I., San, Y., Upper, F., River, S., Cape, A., Dubai, T., Madrid, L., Munich, M., Montreal, P., Delhi, T., São, M. C., Sydney, P., Kong, H., Singapore, S., & Tokyo, T. (2015). *Computer Security Principles and Practice Third Edition.*
- Sugiyono, D. (2013). *Metode penelitian pendidikan: pendekatan kuantitatif, kualitatif, dan R&D.*
- Whitman, M. E., & Mattord, H. J. (2009). *Principles of Information Security.* Thomson Course Technology.
- Williams, A. L., & Merten, M. J. (2008). A review of online social networking profiles by adolescents: implications for future research and intervention. *Adolescence*, 43(170).

LAMPIRAN

Lampiran dalam dokumen ini disusun untuk memberikan informasi tambahan dan pendukung yang mendalam terkait dengan penelitian atau pembahasan utama yang telah diuraikan dalam bab-bab sebelumnya. Lampiran pada penelitian ini adalah sebagai berikut:

- a. Surat permohonan menjadi responden

SURAT PERMOHONAN MENJADI RESPONDEN

Kepada Yth.
Kepala SMPN 1 Ngetos
Di Tempat

Dengan Hormat,

Yang bertanda tangan di bawah ini adalah mahasiswa Program Studi Informatika - Program Sarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia.

Nama : A. Zakki Fikril Maulidi
NIM : 17523234

Akan mengadakan penelitian tentang “**Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk**”. Untuk itu saya mohon kesediaan dari Bapak / Ibu Kepala Sekolah untuk mengizinkan peserta didiknya untuk menjadi responden dalam penelitian ini. Segala hal yang bersifat rahasia akan dirahasiakan dan digunakan hanya untuk penelitian ini.

Demikian surat permohonan ini disampaikan, atas kesediaan siswa siswi sebagai responden saya ucapkan terima kasih.

Nganjuk, 21 Maret 2024

Peneliti,



A Zakki Fikril Maulidi

SURAT PERMOHONAN MENJADI RESPONDEN

Kepada Yth.

Kepala SMP Progresif Baitul Atieq

Di Tempat

Dengan Hormat,

Yang bertanda tangan di bawah ini adalah mahasiswa Program Studi Informatika - Program Sarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia.

Nama : A. Zakki Fikril Maulidi

NIM : 17523234

Akan mengadakan penelitian tentang “ **Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk**”. Untuk itu saya mohon kesediaan dari Ibu Kepala Sekolah untuk mengizinkan peserta didiknya untuk menjadi responden dalam penelitian ini. Segala hal yang bersifat rahasia akan dirahasiakan dan digunakan hanya untuk penelitian ini.

Demikian surat permohonan ini disampaikan, atas kesediaan siswa siswi sebagai responden saya ucapkan terima kasih.

Nganjuk, 21 Maret 2024

Peneliti,



A Zakki Fikril Maulidi

b. Pengisian kuesioner dengan Google Form pada SMPN 1 Ngetos

KUESIONER PENELITIAN TUGAS AKHIR

"Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk"

Penelitian ini dilakukan untuk mengukur tingkat kesadaran keamanan siber pada siswa SMP di Nganjuk. Hasil dari penelitian ini akan dijadikan pedoman untuk mengukur kesadaran keamanan siber pada siswa SMP di Nganjuk berdasarkan faktor demografis siswa.

Perlu disampaikan bahwa hasil kuesioner ini tidak berpengaruh apapun terhadap nilai mata pelajaran. Dengan demikian, mohon dijawab sejujur-jujurnya dan sesuai dengan pemahaman dan keadaan yang sebenarnya. Atas perhatian dan bantuan adik-adik siswa SMP, saya ucapkan terima kasih.

zakifikril80@gmail.com [Ganti akun](#)



Tidak dibagikan

* Menunjukkan pertanyaan yang wajib diisi

I. Identitas Responden

Nama *

Jawaban Anda _____

Kelas *

- 7 (Tujuh)
- 8 (Delapan)
- 9 (Sembilan)

Jenis Kelamin *

- Laki-laki
- Perempuan

Alamat *

Jawaban Anda _____

LEMBAR KUESIONER Kesadaran Keamanan Siber

I. Penggunaan Password

Keterangan : Sangat Tidak Setuju = 1, Tidak Setuju = 2,

Netral / Biasa Saja = 3, Setuju = 4, Sangat Setuju = 5

Saya boleh menggunakan *password* yang sama antara *password* akun media sosial dan selain media sosial (Contoh: akun email, belanja *online*, akun game) *

1 2 3 4 5
Sangat Tidak Setuju Sangat Setuju

Saya boleh membagikan *password* saya kepada teman saya *

1 2 3 4 5
Sangat Tidak Setuju Sangat Setuju

Saya harus menggunakan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus saat membuat *password* *

1 2 3 4 5
Sangat Tidak Setuju Sangat Setuju

Menurut saya, aman-aman saja menggunakan *password* yang sama antara *password* media sosial dengan akun selain media sosial (Contoh: akun email, belanja *online*, akun game) *

1 2 3 4 5
Sangat Tidak Setuju Sangat Setuju

c. Penggunaan lembar kuesioner pada siswa SMP Progresif Baitul Atieq

KUESIONER PENELITIAN TUGAS AKHIR

“ Analisis Kesadaran Keamanan Siber pada Siswa SMP di Nganjuk”

Penelitian ini dilakukan untuk mengukur tingkat kesadaran keamanan siber pada siswa SMP di Nganjuk. Hasil dari penelitian ini akan dijadikan pedoman untuk mengukur kesadaran keamanan siber pada siswa SMP di Nganjuk berdasarkan faktor demografis siswa..

Perlu disampaikan bahwa hasil kuesioner ini tidak berpengaruh apapun terhadap nilai mata pelajaran. Dengan demikian, mohon dijawab sejujur-jujurnya dan sesuai dengan pemahaman dan keadaan yang sebenarnya. Atas perhatian dan bantuan adik-adik siswa SMP, saya ucapkan terima kasih.

I. Identitas Responden

Nama :

Kelas :

Asal Sekolah :

Jenis Kelamin :

Alamat :

.....

Uang saku per hari * : < Rp5000,00

Rp5000,00 - Rp10.000,00

> Rp10.000,00

***(diisi dengan tanda centang √)**

LEMBAR KUESIONER

Kesadaran Keamanan Siber

Keterangan:

STS : Sangat Tidak Setuju

TS : Tidak Setuju

N : Netral / Biasa Saja

S : Setuju

SS : Sangat Setuju

I. Penggunaan Password

No	Pernyataan	STS	TS	N	S	SS
1	Saya boleh menggunakan <i>password</i> yang sama antara <i>password</i> akun media sosial dan selain media sosial (Contoh: akun email, belanja <i>online</i> , akun game)					
2	Saya boleh membagikan <i>password</i> saya kepada teman saya					
3	Saya harus menggunakan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus saat membuat <i>password</i>					
4	Menurut saya, aman-aman saja menggunakan <i>password</i> yang sama antara <i>password</i> media sosial dengan akun selain media sosial (Contoh: akun email, belanja <i>online</i> , akun game)					
5	Membagikan <i>password</i> kepada teman adalah hal buruk, meskipun dengan teman dekat saya					
6	Aman saja menggunakan <i>password</i> yang terdiri dari hanya kombinasi huruf saja					
7	Saya menggunakan <i>password</i> yang berbeda untuk akun media sosial dengan akun selain media sosial (Contoh: akun email, belanja <i>online</i> , akun game)					
8	Saya membagikan <i>password</i> saya kepada teman dekat saya					
9	Saya menggunakan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus untuk semua <i>password</i>					