ANALISIS FAKTOR-FAKTOR YANG MEMENGARUHI PERILAKU KEAMANAN KATA SANDI DI KALANGAN SISWA SMA/SMK SEDERAJAT DI PROVINSI DIY

Disusun Oleh:

N a m a : Bima Panjalu Mukti
NIM : 21523131

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2025

HALAMAN PENGESAHAN DOSEN PEMBIMBING

ANALISIS FAKTOR-FAKTOR YANG MEMENGARUHI PERILAKU KEAMANAN KATA SANDI DI KALANGAN SISWA SMA/SMK SEDERAJAT DI PROVINSI DIY

TUGAS AKHIR

Disusun Oleh:

N a m a : Bima Panjalu Mukti

NIM : 21523131

Yogyakarta, 25 November 2025

Pembimbing 1,	Pembimbing 2,
(Fayruz Rahma, S.T., M.Eng.)	(Moh. Idris, S.Kom., M.Kom.)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS FAKTOR-FAKTOR YANG MEMENGARUHI PERILAKU KEAMANAN KATA SANDI DI KALANGAN SISWA SMA/SMK SEDERAJAT DI PROVINSI DIY

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, 25 November 2025

Tim Penguji

Fayruz Rahma, S.T., M.Eng. _____

Anggota 1

Ahmad Fathan Hidayatullah, S.T., M.Cs. _____

Anggota 2

Erika Ramadhani, S.T., M.Eng. _____

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 : Bima Panjalu Mukti

NIM : 21523131

Tugas akhir dengan judul:

ANALISIS FAKTOR-FAKTOR YANG MEMENGARUHI PERILAKU KEAMANAN KATA SANDI DI KALANGAN SISWA SMA/SMK SEDERAJAT DI PROVINSI DIY

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, 25 November 2025



(Bima Panjalu Mukti)

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim,

Skripsi ini kupersembahkan dengan segenap cinta, syukur, dan kerendahan hati kepada:

1. Ayah dan Ibu tercinta, terima kasih atas doa, dukungan, dan kasih sayang yang tiada henti. Pengorbanan kalian adalah inspirasi terbesarku. Skripsi ini adalah wujud baktiku untukmu.
2. Kedua Kakakku, yang selalu menjadi pilar kekuatan dan motivasi. Terima kasih atas dukungan, nasihat, dan kehangatan yang tak henti.
3. Diri ini, atas segala perjuangan, air mata, dan kerja keras yang telah dilalui. Semoga skripsi ini menjadi awal yang baik untuk perjalanan selanjutnya.

Semoga skripsi ini dapat menjadi amal jariyah dan memberikan manfaat bagi banyak orang.

HALAMAN MOTO

يٰقَوْمِ اِنَّمَا هٰذِهِ الْحَيٰوةُ الدُّنْيَا مَتَاعٌ ۖ وَّاِنَّ الْاٰخِرَةَ هِيَ دَارُ الْقَرَارِ ﴿٣٩﴾

Wahai kaumku! Sesungguhnya kehidupan dunia ini hanyalah kesenangan (sementara) dan sesungguhnya akhirat itulah negeri yang kekal. (QS. Ghâfir/al-Mukmin/40:39)

"Keberhasilan bukanlah milik orang yang pintar, keberhasilan adalah kepunyaan mereka yang senantiasa berusaha"

(B.J Habibie)

"Lebih baik menerima kejujuran yang pahit, daripada kebohongan yang manis."

(Soichiro Yagami)

"Ingatlah bahwa pulih itu tidak selalu kembali seperti dulu, tapi belajar melanjutkan hidup dengan bekas sakitnya"

(Zenitsu Agatsuma)

KATA PENGANTAR

Puji syukur ke hadirat Allah Swt. atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Universitas Islam Indonesia.

Penulisan skripsi dengan judul "Analisis Faktor-Faktor yang Memengaruhi Perilaku Keamanan Kata Sandi di Kalangan Siswa SMA/SMK Sederajat di Provinsi DIY" ini berfokus pada pentingnya kesadaran akan keamanan siber, khususnya dalam penggunaan kata sandi. Di era digital saat ini, kata sandi telah menjadi gerbang utama menuju berbagai layanan *online*, mulai dari media sosial hingga perbankan. Namun, pemahaman dan praktik keamanan kata sandi di kalangan remaja, khususnya siswa SMA/SMK, masih menjadi isu yang krusial. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis faktor-faktor yang memengaruhi perilaku mereka, baik dari sisi pengetahuan, sikap, maupun lingkungan.

Proses penyusunan skripsi ini tidak lepas dari dukungan, bimbingan, dan bantuan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah Swt. atas segala rahmat, nikmat, serta kekuatan yang telah diberikan selama proses penyusunan tugas akhir ini.
2. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia.
3. Bapak Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D. selaku Ketua Program Studi Informatika - Program Sarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia.
4. Ibu Fayruz Rahma, S.T., M.Eng. dan Bapak Moh. Idris, S.Kom., M.Kom. selaku dosen pembimbing yang telah meluangkan waktu, memberikan bimbingan, arahan, dan motivasi yang tak henti-hentinya sejak awal hingga akhir penelitian ini.
5. Ayah, Ibu, dan seluruh keluarga yang selalu memberikan dukungan moral, doa, dan motivasi tanpa batas.
6. Kepala Sekolah, Guru, dan Siswa-siswi SMA/SMK di Provinsi DIY yang telah bersedia menjadi responden dan memberikan data yang sangat berharga untuk penelitian ini.
7. Sahabat-sahabat dan rekan-rekan seperjuangan yang telah memberikan semangat, bantuan, dan kenangan tak terlupakan selama masa perkuliahan.

Penulis menyadari bahwa skripsi ini masih memiliki banyak kekurangan. Oleh karena itu, segala kritik dan saran yang membangun akan diterima dengan senang hati demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat, wawasan, dan kontribusi nyata bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi dan pendidikan.

Yogyakarta, 1 November 2025



(Bima Panjalu Mukti)

SARI

Keamanan kata sandi merupakan aspek penting dalam perlindungan data pribadi di era digital, khususnya bagi siswa SMA dan SMK yang aktif menggunakan teknologi dalam proses belajar dan berinteraksi sosial. Di Provinsi DIY, dengan jumlah siswa mencapai 152.620 pada tahun 2025, isu keamanan digital semakin kompleks akibat rendahnya edukasi kesadaran keamanan di sekolah serta meningkatnya risiko pencurian data dan pembajakan akun.

Penelitian ini bertujuan untuk menganalisis tingkat kesadaran siswa terhadap keamanan kata sandi serta mengidentifikasi faktor-faktor yang memengaruhi perilaku keamanan kata sandi. Penelitian menggunakan pendekatan kuantitatif dengan metode survei terhadap 100 siswa dari empat sekolah di DIY, menggunakan teknik *stratified random sampling*. Data dikumpulkan melalui kuesioner daring berbasis skala Likert lima poin dan dianalisis menggunakan SPSS dan Rstudio. Analisis yang dilakukan meliputi analisis deskriptif, uji validitas dan reliabilitas, uji asumsi klasik, serta regresi linier berganda dengan tingkat signifikansi 10%.

Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan kata sandi siswa tergolong baik (rata-rata 4,12 dari 5), terutama dalam menjaga kerahasiaan kata sandi (4,38) dan penggunaan kombinasi karakter (4,29). Namun, kewaspadaan terhadap tautan mencurigakan masih rendah (3,86). Analisis regresi membuktikan bahwa Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko berpengaruh positif signifikan terhadap Perilaku Keamanan Kata Sandi, dengan Pengalaman Keamanan Siber Pribadi sebagai faktor paling dominan (t-hitung 3,284). Menariknya, variabel Kecemasan Ingatan menunjukkan arah pengaruh positif yang berbeda dari hipotesis awal yang memprediksi hubungan negatif, mengindikasikan bahwa rasa khawatir lupa kata sandi justru mendorong siswa untuk lebih berhati-hati dan cenderung menerapkan praktik keamanan yang lebih baik. Secara keseluruhan, model penelitian ini mampu menjelaskan 15,7% variasi perilaku keamanan kata sandi, sementara 84,3% sisanya dipengaruhi oleh faktor lain.

Kata kunci: keamanan kata sandi, perilaku keamanan siber, siswa SMA/SMK, kecemasan ingatan, pengaruh teman sebaya, pengalaman keamanan siber, persepsi risiko, regresi linier berganda

GLOSARIUM

2FA	Metode keamanan yang mewajibkan dua bentuk verifikasi berbeda, seperti kata sandi dan kode OTP, sebelum pengguna dapat mengakses akun.
Akuntabilitas	Prinsip keamanan informasi yang memastikan setiap tindakan terhadap data atau sistem dapat dilacak dan dipertanggungjawabkan kepada individu atau pihak tertentu.
Akun	Identitas digital pengguna dalam suatu sistem atau platform yang dilindungi oleh kredensial seperti nama pengguna dan kata sandi.
Ancaman Siber	Potensi bahaya yang dapat mengeksploitasi kelemahan sistem untuk mencuri, merusak, atau mengganggu data serta layanan digital.
Autentikasi	Proses verifikasi identitas pengguna untuk memastikan bahwa akses ke sistem hanya diberikan kepada pihak yang sah.
Biometrik	Teknologi autentikasi yang menggunakan karakteristik fisik atau perilaku unik individu, seperti sidik jari, pengenalan wajah, iris mata, atau pola ketikan untuk verifikasi identitas.
Cross-Sectional	Desain penelitian ini merupakan pendekatan yang mengumpulkan data dari responden hanya pada satu waktu tertentu untuk menelaah atau menggambarkan fenomena yang sedang berlangsung pada periode tersebut.
Cybercrime	Tindakan kriminal yang dilakukan melalui teknologi digital, seperti peretasan, penipuan daring, atau pencurian data pribadi.
Cybersecurity	Serangkaian tindakan teknis serta kebijakan yang dibuat dengan tujuan menjaga keamanan sistem komputer, jaringan, dan data dari berbagai ancaman siber.
Denial of Service	Jenis serangan siber yang dilakukan dengan membanjiri sistem menggunakan lalu lintas berlebih sehingga menyebabkan layanan, sistem, atau jaringan tidak dapat diakses oleh pengguna yang berhak.
Enkripsi	Proses mengonversi data ke dalam format terenkripsi sehingga tidak bisa dipahami oleh pihak yang tidak memiliki izin akses.

Explanatory	Penjelasan atau segala sesuatu yang berhubungan dengan kegiatan memberikan keterangan, baik mengenai peristiwa yang sedang terjadi maupun keadaan yang diperkirakan akan terjadi di masa depan.
Firewall	Sistem keamanan jaringan yang berfungsi mengendalikan arus data yang masuk maupun keluar guna mencegah terjadinya akses tanpa izin.
Frasa Sandi	Jenis kata sandi yang terdiri dari rangkaian kata yang panjang dan mudah diingat, tetapi sulit ditebak, yang menawarkan tingkat keamanan lebih tinggi dibandingkan kata sandi konvensional.
Hacker	Individu yang memiliki keahlian teknis dalam bidang komputer dan jaringan yang berupaya mendapatkan akses tidak sah ke sistem atau data dengan mengeksploitasi kelemahan keamanan.
Kontrol Akses	Mekanisme keamanan yang membatasi dan mengatur siapa yang dapat mengakses sumber daya tertentu dalam sistem informasi berdasarkan kebijakan yang telah ditetapkan.
Password Manager	Aplikasi yang digunakan untuk menyimpan dan mengelola kata sandi secara terenkripsi agar lebih aman dan mudah diakses.
Phishing	Upaya penipuan daring dengan menyamar sebagai pihak tepercaya untuk mencuri informasi sensitif seperti kata sandi atau data pribadi.
Pola (*Pattern*)	Jenis autentikasi yang menggunakan urutan titik atau garis yang digambar pada layar sentuh perangkat sebagai pengganti kata sandi tradisional.
Ransomware	Perangkat lunak berbahaya yang mengunci atau mengenkripsi data milik korban dan meminta pembayaran tebusan agar akses terhadap data tersebut dapat dipulihkan.
Self-Efficacy	Keyakinan seseorang terhadap kemampuan dirinya dalam melakukan tindakan tertentu, misalnya dalam menjaga keamanan akun digital.
Self-Report	Metode pengumpulan data di mana responden melaporkan sendiri informasi tentang diri mereka, seperti sikap, perilaku, atau pengalaman melalui kuesioner atau wawancara.

Spyware	Jenis *malware* yang dirancang untuk memperoleh data atau informasi mengenai pengguna maupun organisasi tanpa sepengetahuan mereka, kemudian mengirimkan data tersebut kepada pihak ketiga.
SQL Injection	Teknik serangan siber yang mengeksploitasi kerentanan dalam aplikasi web dengan menyisipkan kode SQL berbahaya untuk mengakses atau memanipulasi *database*.
Trojan	Jenis *malware* yang menyamar sebagai program yang sah atau bermanfaat tetapi sebenarnya berbahaya dan dapat memberikan akses tidak sah kepada penyerang.
Virus	Jenis *malware* yang dapat mereplikasi diri dan menyebar ke program atau file lain dengan cara menyisipkan kode berbahaya, sering kali menyebabkan kerusakan pada sistem.
Worm	Jenis *malware* yang dapat mereplikasi diri dan menyebar melalui jaringan tanpa memerlukan interaksi pengguna atau file host, biasanya mengeksploitasi kerentanan keamanan.

DAFTAR ISI

HALAMAN JUDUL 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 ix
GLOSARIUM x
DAFTAR ISI xiii
DAFTAR TABEL xv
DAFTAR GAMBAR xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Batasan Penelitian 3
1.5 Manfaat Penelitian 4
1.6 Metodologi Penelitian 5
1.7 Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA 7
2.1 Keamanan Informasi 7
2.1.1 Pengertian dan Prinsip Dasar Keamanan Informasi 7
2.1.2 Ancaman terhadap Keamanan Informasi 8
2.1.3 Praktik Terbaik dalam Keamanan Informasi 9
2.2 Keamanan Kata Sandi 9
2.2.1 Konsep Dasar Kata Sandi 9
2.2.2 Ancaman Keamanan Kata Sandi 10
2.2.3 Praktik Terbaik dalam Pengamanan Kata Sandi 10
2.3 Perilaku Keamanan Informasi di Kalangan Siswa SMA/SMK 11
2.4 Perangkat Analisis Data 13
2.4.1 RStudio 13
2.4.2 IBM SPSS Statistics 13
2.5 Analisis Deskriptif 14
2.6 Asumsi Klasik 14
2.7 Regresi Linier Berganda 15
2.7.1 Konsep Dasar Analisis Regresi Linier Berganda 15
2.7.2 Interpretasi Hasil Analisis Regresi Linier Berganda 16
2.7.3 Penelitian Terkait Regresi Linier Berganda dalam Konteks Keamanan Informasi 16
2.8 Skala Likert 17
2.9 Penelitian Terdahulu dan Kesenjangan Penelitian 17
BAB III METODOLOGI PENELITIAN 22
3.1 Metode Penelitian 24
3.2 Jenis dan Pendekatan Penelitian 25
3.3 Populasi dan Sampel 25
3.3.1 Populasi 25

3.3.2 Sampel....25
3.4 Teknik Penentuan Sampel....27
3.5 Instrumen Penelitian....28
3.6 Lokasi dan Waktu Penelitian....31
3.7 Variabel Penelitian....32
3.7.1 Variabel Independen (X)....32
3.7.2 Variabel Dependen (Y)....33
3.7.3 Kerangka Hubungan Antarvariabel....34
3.8 Hipotesis Penelitian....34
3.9 Metode Pengumpulan Data....37
3.10 Alat Analisis Data....37
3.10.1 RStudio....37
3.10.2 IBM SPSS Statistics 31....37
3.11 Validasi Instrumen Penelitian....38
3.12 Analisis Deskriptif....39
3.13 Uji Asumsi Klasik....39
3.14 Uji Analisis Data....41
BAB IV HASIL PENELITIAN DAN PEMBAHASAN....43
4.1 Hasil Analisis Deskripstif....43
4.1.1 Karakteristik Responden Berdasarkan Asal Sekolah....43
4.1.2 Karakteristik Responden Berdasarkan Jenis Kelamin....43
4.1.3 Karakteristik Responden Berdasarkan Usia....44
4.1.4 Karakteristik Responden Berdasarkan Tingkat Kelas....45
4.1.5 Analisis Tingkat Kesadaran Keamanan Kata Sandi pada Siswa SMA/SMK....45
4.2 Validasi Intrumen Penelitian....47
4.3 Uji Asumsi Klasik....53
4.3.1 Uji Normalitas....54
4.3.2 Uji Linearitas....55
4.3.3 Uji Multikolinearitas....58
4.3.4 Uji Heteroskedastisitas....59
4.4 Analisis Regresi Linier Berganda....60
4.4.1 Uji Simultan (Uji-f)....63
4.4.2 Uji Parsial (Uji-t)....64
4.4.3 Koefisien Determinasi ($\boldsymbol{R2}$)....67
4.5 Interpretasi Hasil Penelitian....67
BAB V KESIMPULAN DAN SARAN....69
5.1 Kesimpulan....69
5.2 Saran....70
DAFTAR PUSTAKA....71
LAMPIRAN A....78
LAMPIRAN B....84
LAMPIRAN C....85
LAMPIRAN D....87

DAFTAR TABEL

Tabel 2. 1 Skala Likert 17
Tabel 2. 2 Hasil Temuan Penelitian Terdahulu dan Kesenjangan Penelitian 18
Tabel 3. 1 Operasionalisasi Variabel Penelitian 29
Tabel 3. 2 Skala Likert untuk Penyataan Positif dan Negatif 31
Tabel 4. 1 Kesimpulan Hasil Analisis Variabel Perilaku Kemanana Kata Sandi 46
Tabel 4. 2 Hasil Kesimpulan Uji Validitas 50
Tabel 4. 3 Kesimpulan Uji Reliabilitas 53
Tabel 4. 4 Kesimpulan Uji Linearitas SPSS 56
Tabel 4. 5 Hasil Kesimpulan Analisis Regresi Linier Berganda 62
Tabel 4. 6 Hasil Koefisien Determinasi dan Uji F dengan Regresi Linier Berganda 63

DAFTAR GAMBAR

Gambar 3. 1 Diagram Alur Penelitian 22
Gambar 3. 2 Hubungan Antarvariabel 34
Gambar 4. 1 Diagram *Pie* Asal Sekolah 43
Gambar 4. 2 Diagram *Pie* Jenis Kelamin 44
Gambar 4. 3 Diagram *Pie* Usia 44
Gambar 4. 4 Diagram *Pie* Tingkat Kelas 45
Gambar 4. 5 Analisis Deskriptif Variabel Perilaku Keamanan Kata Sandi 45
Gambar 4. 6 Diagram Batang Rata-rata Variabel Perilaku Kemanana Kata Sandi 46
Gambar 4. 7 Hasil semua Variabel dari Uji Validitas dengan RStudio 47
Gambar 4. 8 Hasil Uji Validitas Variabel Kecemasan Ingatan dengan SPSS 48
Gambar 4. 9 Hasil Uji Validitas Variabel Pengaruh Teman Sebaya dengan SPSS 48
Gambar 4. 10 Hasil Uji Validitas Variabel Perilaku Keamanan Siber Pribadi dengan SPSS 49
Gambar 4. 11 Hasil Uji Validitas Variabel Persepsi Risiko dengan SPSS 49
Gambar 4. 12 Hasil Uji Validitas Variabel Perilaku Keamanan Kata Sandi dengan SPSS 50
Gambar 4. 13 Hasil Uji Reliabilitas dengan SPSS 52
Gambar 4. 14 Hasil Uji Reliabilitas dengan RStudio 52
Gambar 4. 15 Hasil Uji Normalitas dengan SPSS 54
Gambar 4. 16 Grafik Q-Q Residual Plot Uji Normalitas dengan SPSS 54
Gambar 4. 17 Hasil Uji Normalitas dengan RStudio 54
Gambar 4. 18 Grafik Q-Q Plot Residual Uji Normalitas dengan RStudio 55
Gambar 4. 19 Uji Linearitas menggunakan SPSS 56
Gambar 4. 20 Grafik Uji Linearitas menggunakan RStudio 57
Gambar 4. 21 Hasil Uji Multikolinearitas dengan SPSS 58
Gambar 4. 22 Hasil Uji Multikolinearitas dengan RStudio 58
Gambar 4. 23 Hasil Uji Heteroskedastisitas dengan SPSS 59
Gambar 4. 24 Hasil Uji Heteroskedastisitas dengan RStudio 60
Gambar 4. 25 Hasil Analisis Regresi Linier Berganda menggunakan SPSS 61
Gambar 4. 26 Hasil Analisis Regresi Linier Berganda menggunakan RStudio 61
Gambar 4. 27 Hasil Uji Koefisien Determinasi menggunakan SPSS 67

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan siber merupakan aspek yang sangat berpengaruh dalam kehidupan digital saat ini, terutama dengan semakin tingginya keterlibatan masyarakat dalam aktivitas daring. Keamanan siber mencakup berbagai teknologi dan metode untuk melindungi data, mencegah akses tidak sah, gangguan, atau pengungkapan informasi pribadi yang sensitif. Dengan pesatnya perkembangan teknologi, ancaman siber menjadi salah satu tantangan yang paling signifikan, yang dapat merusak integritas data dan sistem digital. Oleh karena itu, pemahaman yang mendalam tentang keamanan siber sangat penting untuk mengurangi potensi kerugian akibat serangan dunia maya (Alrobaian et al., 2023; Saeed, 2023).

Salah satu masalah yang paling sering ditemukan dalam praktik keamanan siber adalah pengelolaan kata sandi yang tidak memadai. Banyak pengguna masih menggunakan kata sandi yang lemah atau mengulang kombinasi yang sama pada berbagai akun mereka sehingga membuka celah bagi peretas untuk mengekspos informasi pribadi mereka. Meskipun sudah banyak program pelatihan yang dilakukan, riset menunjukkan bahwa banyak individu yang masih kesulitan untuk mengimplementasikan praktik keamanan ini dalam kehidupan sehari-hari mereka. Hal ini menunjukkan bahwa perlu ada pendekatan yang lebih efektif dalam mendidik masyarakat untuk lebih konsisten dalam menerapkan keamanan siber (Kennison & Chan-Tin, 2020; Santyadiputra & Kustono, 2023). Perbedaan antara pengetahuan dan penerapan ini menjadi salah satu isu utama dalam menjaga keamanan di dunia maya.

Keamanan siber juga menjadi perhatian yang sangat penting di kalangan siswa Sekolah Menengah Atas (SMA) dan Sekolah Menengah Kejuruan (SMK), terutama karena mereka sangat bergantung pada teknologi dalam kegiatan belajar mereka. Penelitian yang dilakukan oleh (Titiakarawongse & Boonkrong, 2023) mengungkapkan bahwa meskipun siswa memiliki pemahaman dasar tentang cara membuat *password* yang kompleks, perilaku mereka masih sering membuat mereka rentan terhadap serangan siber. Hal ini menunjukkan bahwa ada kebutuhan mendesak untuk memperkuat pendidikan tentang keamanan siber di kalangan siswa SMA/SMK agar mereka dapat melindungi diri mereka dari berbagai risiko digital yang ada (Blažič & Blažič, 2022; Peker et al., 2018).

Keamanan informasi menjadi isu yang semakin krusial, terutama di kalangan remaja yang aktif menggunakan teknologi dalam kegiatan pembelajaran dan interaksi sosial sehari-hari. Di Provinsi Daerah Istimewa Yogyakarta, dengan total 225 SMA dan 187 SMK serta jumlah siswa mencapai 152.620 orang pada tahun 2025 (Kementerian Pendidikan Dasar dan Menengah, 2025), tantangan keamanan digital menjadi semakin kompleks, terutama dalam aspek pengelolaan kata sandi sebagai garis pertahanan pertama keamanan data. Kondisi ini semakin mengkhawatirkan mengingat tingginya risiko pelanggaran keamanan di dunia pendidikan, dengan 32% kasus berujung pada pencurian data dan 27% mengalami pembajakan (Mamduh Mohamad, 2024). Fakta ini tercermin dari hanya 14% sekolah yang mewajibkan pelatihan kesadaran keamanan (Mamduh Mohamad, 2024).

Tantangan keamanan digital di kalangan pelajar tersebut menegaskan pentingnya pemahaman terhadap perilaku pengguna dalam menjaga keamanan melalui penggunaan kata sandi. Penelitian Hadzidedic et al. (2022) menunjukkan bahwa persepsi pengguna terhadap metode autentikasi, termasuk kata sandi, berpengaruh besar terhadap tingkat keamanan yang diterapkan. Poornachandran et al. (2016) juga menemukan bahwa meskipun siswa menyadari pentingnya keamanan kata sandi, banyak yang masih menggunakan kata sandi yang lemah atau mengulang kata sandi yang sama untuk berbagai akun sehingga meningkatkan risiko kebocoran data pribadi. Studi Booc et al. (2024) mengenai kesadaran siber di kalangan siswa SMA menemukan bahwa meskipun tingkat kesadaran cukup tinggi, perilaku keamanan mereka masih membutuhkan perhatian lebih. Temuan ini diperkuat oleh penelitian Moallem (2019) yang menunjukkan bahwa kesadaran akan risiko belum tentu berujung pada tindakan pencegahan yang efektif. Di sisi lain, Sulaiman et al. (2022) menekankan pentingnya motivasi untuk melindungi diri dalam membentuk perilaku yang lebih baik terkait keamanan siber.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk mengidentifikasi faktor-faktor yang memengaruhi perilaku terkait keamanan kata sandi di kalangan siswa SMA/SMK di Provinsi Daerah Istimewa Yogyakarta (DIY). Pemilihan lokasi ini dianggap strategis karena Provinsi DIY memiliki keberagaman latar belakang siswa yang mencerminkan kondisi pendidikan yang dinamis. Diharapkan, hasil penelitian ini dapat memberikan wawasan yang lebih dalam mengenai pola perilaku keamanan kata sandi siswa serta faktor-faktor yang memengaruhinya. Temuan ini nantinya akan berguna dalam mengembangkan program edukasi keamanan siber yang lebih efektif, serta merancang kebijakan keamanan informasi yang lebih sesuai dengan karakteristik dan kebutuhan siswa.

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang masalah, maka dapat disimpulkan permasalahan yang akan dibahas pada penelitian ini adalah:

a. Bagaimana tingkat kesadaran siswa SMA/SMK di Provinsi DIY terhadap pentingnya keamanan kata sandi dalam kehidupan digital?
b. Apa saja faktor-faktor yang memengaruhi perilaku keamanan kata sandi di kalangan siswa SMA/SMK di Provinsi DIY?

1.3 Tujuan Penelitian

Berdasarkan dari uraian rumusan masalah di atas, tujuan dari penelitian ini adalah:

a. Menganalisis faktor-faktor yang memengaruhi perilaku keamanan kata sandi di kalangan siswa SMA/SMK di Provinsi DIY.
b. Menganalisis dan mengukur tingkat kesadaran siswa SMA/SMK di Provinsi DIY mengenai pentingnya keamanan siber dalam aktivitas digital mereka sehari-hari.

1.4 Batasan Penelitian

Untuk menjaga fokus dan relevansi penelitian agar tidak meluas dari permasalahan yang dikaji, ditetapkan beberapa batasan agar hasil yang diperoleh tetap selaras dengan tujuan penelitian. Adapun batasan penelitian ini adalah sebagai berikut.

a. Penelitian ini memiliki batasan geografis yang difokuskan pada siswa SMA/SMK sederajat yang bersekolah di Provinsi DIY. Dengan demikian, hasil penelitian ini tidak dapat digeneralisasikan untuk siswa di provinsi lain, mengingat adanya potensi perbedaan dalam karakteristik demografis, tingkat literasi digital, serta akses terhadap teknologi informasi yang bervariasi antar wilayah di Indonesia.
b. Penelitian ini hanya mencakup empat faktor yang diduga berpengaruh terhadap perilaku keamanan kata sandi, yaitu kecemasan ingatan, pengaruh teman sebaya, pengalaman keamanan siber pribadi, dan persepsi risiko. Peneliti menyadari bahwa masih terdapat faktor-faktor lain yang berpotensi memengaruhi perilaku keamanan kata sandi, seperti tingkat pengetahuan keamanan siber, dukungan orang tua, kurikulum pendidikan digital di sekolah, maupun karakteristik kepribadian individu, yang belum dianalisis dalam penelitian ini.
c. Pengumpulan data dalam penelitian ini dilakukan melalui instrumen kuesioner dengan metode *self-report*, yang bergantung pada tingkat kejujuran serta kemampuan responden dalam mengingat dan melaporkan perilaku mereka sendiri. Metode ini memiliki keterbatasan karena berpotensi menimbulkan bias respons, seperti *social desirability* bias,

di mana responden cenderung memberikan jawaban yang dianggap lebih dapat diterima secara sosial dibandingkan dengan perilaku sebenarnya.

d. Penelitian ini menggunakan desain *cross-sectional*, di mana pengumpulan data dilakukan hanya pada satu waktu tertentu. Desain penelitian ini membatasi kemampuan peneliti untuk menjelaskan hubungan kausal antarvariabel maupun mengamati perubahan perilaku keamanan kata sandi dari waktu ke waktu. Oleh karena itu, dinamika perilaku yang mungkin berubah seiring dengan perkembangan usia, pengalaman, atau kondisi lingkungan tidak dapat diidentifikasi secara komprehensif melalui penelitian ini.

e. Penelitian ini berfokus pada kelompok responden siswa tingkat SMA/SMK sederajat, sehingga hasil penelitian tidak dapat digeneralisasikan pada kelompok usia atau jenjang pendidikan lainnya. Kemungkinan terdapat perbedaan karakteristik dan pola perilaku keamanan kata sandi antara kelompok pelajar yang lebih muda maupun individu dengan tingkat pendidikan yang lebih tinggi.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat atau kontribusi sebagai berikut:

a. Teoretis

1. Memberikan kontribusi pada pengembangan ilmu pengetahuan dalam bidang keamanan siber, khususnya dalam konteks pendidikan kejuruan di Indonesia.
2. Penelitian ini juga dapat memperkaya kajian tentang faktor-faktor yang memengaruhi praktik keamanan digital di kalangan generasi muda.

b. Praktis

Temuan penelitian ini dapat dimanfaatkan oleh sekolah maupun lembaga pendidikan sebagai dasar dalam merancang program pembelajaran dan pelatihan yang bertujuan meningkatkan perilaku siswa tentang pentingnya menjaga keamanan kata sandi. Selain itu, hasil penelitian ini juga dapat dijadikan referensi dalam penyusunan kebijakan yang lebih efektif untuk melindungi data pribadi serta informasi siswa dari ancaman siber.

1.6 Metodologi Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei untuk menganalisis faktor-faktor yang memengaruhi perilaku keamanan kata sandi di kalangan siswa SMA/SMK sederajat di Provinsi DIY. Populasi penelitian adalah siswa SMA/SMK di Provinsi DIY dengan sampel sebanyak 100 siswa yang berasal dari empat sekolah berbeda, yaitu SMA Negeri 2 Wonosari, SMA Muhammadiyah 1 Prambanan, SMK Muhammadiyah 1 Wates, dan SMK Negeri 6 Yogyakarta. Teknik pengambilan sampel menggunakan *stratified random sampling* dengan kriteria siswa aktif yang menggunakan akun digital untuk keperluan sekolah dan media sosial.

Pengumpulan data dilakukan melalui kuesioner daring yang disebarkan menggunakan platform *Google Forms*. Instrumen penelitian terdiri dari lima variabel utama yang diukur menggunakan skala Likert lima poin, meliputi empat variabel independen yaitu Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko, serta satu variabel dependen yaitu Perilaku Keamanan Kata Sandi. Sebelum dilakukan analisis, instrumen penelitian diuji terlebih dahulu menggunakan uji validitas dan uji reliabilitas untuk memastikan kualitas data yang dikumpulkan.

Analisis data dilakukan menggunakan dua perangkat lunak statistik yaitu RStudio Build 496 dan IBM SPSS Statistics versi 31. Tahapan analisis meliputi analisis statistik deskriptif untuk menggambarkan karakteristik responden dan tingkat kesadaran keamanan kata sandi, uji asumsi klasik yang mencakup uji normalitas, uji linearitas, uji multikolinearitas, dan uji heteroskedastisitas untuk memastikan kelayakan model regresi, serta analisis regresi linier berganda untuk menguji pengaruh variabel independen terhadap variabel dependen. Pengujian hipotesis dilakukan melalui uji simultan atau uji F untuk mengetahui pengaruh seluruh variabel independen secara bersama-sama dan uji parsial atau uji t untuk mengetahui pengaruh masing-masing variabel independen secara individual terhadap perilaku keamanan kata sandi, dengan tingkat signifikansi yang ditetapkan sebesar sepuluh persen atau alpha sama dengan nol koma sepuluh.

1.7 Sistematika Penulisan

Penelitian ini disusun secara sistematis ke dalam lima bab yang saling berkaitan untuk memberikan pemahaman menyeluruh mengenai faktor-faktor yang memengaruhi perilaku keamanan kata sandi di kalangan siswa SMA/SMK di Provinsi DIY. Adapun sistematika penulisannya adalah sebagai berikut.

a. **Bab I Pendahuluan** berisi gambaran umum penelitian yang mencakup latar belakang masalah mengenai pentingnya keamanan kata sandi di era digital, rumusan masalah, tujuan, dan manfaat penelitian baik secara teoretis maupun praktis. Bab ini juga menjelaskan secara singkat metode penelitian yang digunakan serta sistematika penulisan keseluruhan laporan penelitian.
b. **Bab II Tinjauan Pustaka** membahas teori dan konsep yang relevan, mulai dari keamanan informasi, keamanan kata sandi, hingga perilaku keamanan informasi di kalangan siswa SMA/SMK. Bab ini juga menjelaskan perangkat analisis data yang digunakan (IBM SPSS Statistics 31 dan RStudio), konsep analisis deskriptif dan regresi linier berganda, skala Likert sebagai instrumen pengukuran, serta kajian penelitian terdahulu dan kesenjangan penelitian yang menjadi dasar pengembangan studi ini.
c. **Bab III Metodologi Penelitian** menjelaskan rancangan penelitian yang digunakan, meliputi jenis dan pendekatan kuantitatif, populasi dan sampel penelitian, teknik penentuan sampel, instrumen penelitian, lokasi dan waktu penelitian, variabel penelitian, hipotesis penelitian, metode pengumpulan data, alat analisis data, serta uji validitas dan reliabilitas. Selain itu, bab ini menjabarkan uji asumsi klasik, serta metode analisis seperti regresi linier berganda yang mencakup uji F, uji t, dan koefisien determinasi.
d. **Bab IV Hasil Penelitian dan Pembahasan** memaparkan hasil analisis data serta interpretasinya. Bab ini mencakup karakteristik responden, hasil analisis deskriptif, uji validitas dan reliabilitas, uji asumsi klasik, hasil regresi linier berganda, uji simultan dan parsial, serta analisis koefisien determinasi. Selanjutnya, hasil penelitian dibahas dengan mengaitkannya pada teori dan penelitian terdahulu untuk menilai kesesuaian serta implikasi dari temuan yang diperoleh.
e. **Bab V Penutup** berisi kesimpulan dan saran. Kesimpulan merangkum hasil utama penelitian terkait tingkat kesadaran siswa dan faktor-faktor yang memengaruhi perilaku keamanan kata sandi. Sementara itu, saran ditujukan kepada sekolah, pemerintah, peneliti, serta siswa agar hasil penelitian ini dapat dimanfaatkan untuk meningkatkan kesadaran dan praktik keamanan kata sandi di kalangan pelajar SMA/SMK di Provinsi DIY.

BAB II
TINJAUAN PUSTAKA

Bab ini menyajikan eksplorasi komprehensif terhadap literatur yang relevan dengan fokus penelitian mengenai perilaku keamanan kata sandi di kalangan siswa SMA/SMK. Kajian ini disusun secara sistematis, dimulai dari konseptualisasi fundamental keamanan informasi, dilanjutkan dengan elaborasi spesifik mengenai keamanan kata sandi, serta analisis mendalam terhadap perilaku keamanan informasi dalam konteks siswa SMA/SMK.

2.1 Keamanan Informasi

2.1.1 Pengertian dan Prinsip Dasar Keamanan Informasi

Keamanan informasi merupakan aspek yang sangat vital dalam dunia digital saat ini. Secara umum, keamanan informasi merujuk pada langkah-langkah yang diambil untuk melindungi data dan informasi dari ancaman yang berasal dari pihak yang tidak berwenang (Mokodompit & Nurlaela, 2017; Novianto et al., 2023; Safitri et al., 2020).

Prinsip-prinsip utama dalam menjaga keamanan informasi meliputi:

1. Kerahasiaan (*Confidentiality*): Memastikan bahwa akses hanya diberikan kepada individu atau pihak yang memiliki otorisasi terhadap informasi tersebut (Mokodompit & Nurlaela, 2017; Safitri et al., 2020).
2. Integritas (*Integrity*): Menjamin bahwa informasi tidak mengalami perubahan atau manipulasi oleh pihak yang tidak berwenang (Mokodompit & Nurlaela, 2017; Safitri et al., 2020).
3. Ketersediaan (*Availability*): Memastikan bahwa informasi dapat diakses dan digunakan oleh pihak yang berwenang sesuai kebutuhan (Mokodompit & Nurlaela, 2017; Safitri et al., 2020).
4. Akuntabilitas (*Accountability*): Setiap tindakan terkait informasi harus dapat dipertanggungjawabkan dengan jelas (Albone, 2009).
5. Autentikasi (*Authentication*): Memastikan bahwa individu yang mengakses informasi adalah pihak yang sah dan terotorisasi (Putri et al., 2023).

Untuk menerapkan prinsip-prinsip tersebut, berbagai pendekatan dan standar dapat digunakan, di antaranya:

1. Penggunaan teknologi keamanan seperti enkripsi, *firewall*, dan sistem deteksi intrusi (Novianto et al., 2023).
2. Implementasi manajemen risiko informasi dengan pendekatan seperti *OCTAVE Allegro* (Deva & Jayadi, 2022).
3. Penggunaan teknik-teknik pengamanan jaringan, seperti *port knocking* dan *port blocking* (Putri et al., 2023).
4. Penerapan prinsip *defense in depth*, yaitu penggunaan beberapa lapisan keamanan untuk perlindungan yang lebih maksimal (Novianto et al., 2023).

Dengan mengadopsi berbagai metode ini, organisasi dapat meningkatkan ketahanan dan integritas sistem informasi mereka dalam menghadapi potensi ancaman yang semakin kompleks.

2.1.2 Ancaman terhadap Keamanan Informasi

1. *Malware* merujuk pada perangkat lunak yang sengaja dirancang untuk merusak, mengganggu, atau memberikan akses tanpa izin ke sistem komputer. Contoh *malware* termasuk *virus*, *worm*, *trojan*, *spyware*, dan *ransomware*. Serangan ini dapat menyebabkan kerusakan pada data, pencurian informasi, serta gangguan terhadap kelancaran operasional sistem (Dwi Madya et al., 2023; Fitria, 2023; Muhazzab et al., 2023).
2. Serangan hacker melibatkan upaya pihak yang tidak berwenang untuk mendapatkan akses ilegal ke dalam sistem atau data. Para hacker sering memanfaatkan celah atau kelemahan dalam sistem keamanan untuk mengambil alih kendali. Dampaknya bisa berupa pencurian data, kerusakan sistem, serta gangguan pada proses operasional organisasi (Muhazzab et al., 2023).
3. Pencurian data terjadi ketika seseorang secara ilegal mengakses dan mencuri informasi tanpa izin. Metode yang digunakan bisa beragam, seperti serangan siber, social engineering, atau bahkan akses fisik yang tidak sah. Konsekuensinya termasuk kebocoran informasi sensitif, kerugian finansial, serta kerusakan reputasi perusahaan (Dwi Madya et al., 2023; Fitria, 2023; Muhazzab et al., 2023).

4. Selain *malware* dan serangan hacker, terdapat ancaman siber lainnya seperti SQL injection, serangan denial of service (DoS), phishing, dan social engineering. Serangan-serangan ini memanfaatkan celah dalam sistem, proses, atau kelalaian manusia untuk merusak, mengakses, atau mengganggu operasional sistem. Dampak yang ditimbulkan bisa berupa kehilangan data, gangguan operasional, dan kerugian finansial (Muhazzab et al., 2023).

2.1.3 Praktik Terbaik dalam Keamanan Informasi

Untuk menghadapi berbagai ancaman keamanan informasi, individu perlu menerapkan serangkaian langkah pengamanan yang efektif, seperti (Raharjo, 2021):

1. Enkripsi Data untuk melindungi informasi agar tidak dapat diakses tanpa izin.
2. Autentikasi pengguna merupakan langkah penting dalam memastikan bahwa individu yang mencoba mengakses suatu sistem benar-benar memiliki hak dan otorisasi yang sesuai.
3. Penggunaan *One-Time Password* (OTP), yaitu kode sandi sekali pakai yang pertama kali diperkenalkan pada tahun 1980. Mekanisme ini meningkatkan keamanan dengan memastikan bahwa meskipun kata sandi utama diketahui pihak lain, akses tetap tidak dapat dilakukan tanpa verifikasi tambahan melalui faktor kedua.
4. Kontrol Akses yang membatasi siapa yang dapat mengakses data atau sistem tertentu.
5. Backup Data untuk memastikan pemulihan data yang hilang akibat ancaman atau kerusakan.

2.2 Keamanan Kata Sandi

2.2.1 Konsep Dasar Kata Sandi

Keamanan *password* memainkan peran yang sangat krusial dalam melindungi informasi sensitif dari ancaman siber. Berikut adalah beberapa jenis *password* yang umum digunakan:

1. *Password* Konvensional (Kata Sandi)

   Password konvensional adalah bentuk *password* yang paling banyak digunakan. *Password* ini biasanya terdiri dari kombinasi huruf, angka, dan simbol yang dipilih oleh pengguna. Tingkat keamanannya sangat bergantung pada kompleksitas dan keunikannya (Flowerday, 2021; Luna, 2019).

2. Frasa Sandi (*Passphrase*)

Frasa sandi merupakan jenis *password* yang terdiri dari rangkaian kata yang mudah diingat oleh pengguna (Bhana & Flowerday, 2021; Luna, 2019). Dibandingkan dengan *password* biasa, frasa sandi lebih sulit untuk ditebak dan menawarkan tingkat keamanan yang lebih tinggi (Bhana & Flowerday, 2021; Luna, 2019).

2.2.2 Ancaman Keamanan Kata Sandi

Kata sandi berfungsi sebagai lapisan pertahanan utama dalam melindungi informasi digital. Namun, efektivitasnya sering kali menurun akibat kebiasaan pengguna yang kurang tepat dalam membuat, menyimpan, dan mengelola kata sandi. Beberapa ancaman umum terhadap keamanan kata sandi dapat dijelaskan sebagai berikut (Walters & Matulich, 2009).

1. Banyak pengguna cenderung memilih kata sandi yang mudah diingat agar praktis digunakan. Sayangnya, kata sandi semacam ini biasanya juga mudah ditebak atau diretas, sehingga menjadi target empuk bagi pelaku kejahatan siber.
2. Sebagian pengguna masih memiliki kebiasaan menuliskan kata sandi mereka di tempat yang mudah terlihat, seperti di layar monitor, meja kerja, atau di bawah keyboard. Praktik ini sangat berisiko karena memungkinkan pihak lain dengan mudah mengakses informasi tersebut secara langsung tanpa perlu meretas sistem.
3. Ketika diminta untuk mengganti kata sandi secara berkala, pengguna sering kali hanya melakukan sedikit modifikasi terhadap kata sandi lama, misalnya dengan menambahkan angka atau huruf di belakangnya. Pola semacam ini menimbulkan risiko tinggi karena mudah ditebak, terutama jika kata sandi sebelumnya sudah diketahui oleh pihak lain.
4. Ancaman lain berasal dari pengelolaan kata sandi yang tidak memadai, seperti tidak menerapkan kebijakan perubahan kata sandi secara berkala, tidak menonaktifkan akun yang sudah tidak digunakan, atau memiliki prosedur pengaturan ulang kata sandi yang lemah. Kondisi ini dapat membuka peluang terjadinya akses tidak sah terhadap sistem atau data sensitif.

2.2.3 Praktik Terbaik dalam Pengamanan Kata Sandi

Untuk menjaga keamanan informasi, berikut adalah beberapa praktik terbaik yang dapat diterapkan dalam pengamanan *password* (Bhana & Flowerday, 2021; Kennison & Chan-Tin, 2020; Luna, 2019):

1. Gunakan *password* yang kompleks dan unik untuk setiap akun.
2. Hindari penggunaan informasi pribadi yang mudah ditebak, seperti nama atau tanggal lahir.
3. Perbarui *password* secara berkala untuk mengurangi risiko kebocoran data.
4. Jangan simpan *password* dalam bentuk teks biasa di perangkat atau aplikasi.
5. Hindari penggunaan fitur "ingat sandi" pada peramban *web*, yang dapat memudahkan akses tidak sah.
6. Terapkan autentikasi dua faktor (*2FA*) untuk meningkatkan lapisan keamanan.
7. Edukasikan pengguna tentang pentingnya menjaga keamanan *password* untuk mengurangi potensi kebocoran data.

2.3 Perilaku Keamanan Informasi di Kalangan Siswa SMA/SMK

Perilaku keamanan informasi di kalangan siswa SMA dan SMK menjadi isu yang semakin penting seiring dengan pesatnya perkembangan teknologi digital di era ini. Penggunaan internet yang semakin meluas di kalangan remaja menjadikan pemahaman terhadap keamanan informasi sebagai hal yang sangat krusial. Melindungi data pribadi serta menghindari risiko-risiko terkait dengan aktivitas *online* menjadi tantangan besar bagi generasi muda. Oleh karena itu, pemahaman dan penerapan perilaku keamanan informasi yang tepat di kalangan siswa SMA/SMK perlu ditingkatkan melalui berbagai upaya edukasi dan kebijakan yang lebih efektif.

Untuk memahami lebih dalam mengenai cara perilaku keamanan informasi terbentuk di kalangan siswa, diperlukan kajian terhadap karakteristik yang memengaruhi perilaku tersebut. Karakteristik perilaku siswa SMA/SMK dalam hal keamanan informasi mencakup beberapa aspek penting yang berkaitan dengan pemahaman mereka terhadap ancaman keamanan siber, kesadaran akan potensi risiko, serta langkah-langkah yang diambil untuk melindungi diri dari bahaya tersebut. Beberapa karakteristik utama yang dapat diidentifikasi di antaranya adalah:

1. Tingkat Kesadaran Terhadap Keamanan Siber

   Siswa SMA/SMK menunjukkan tingkat kesadaran yang bervariasi mengenai keamanan siber. Meskipun mereka aktif dalam menggunakan internet dan media sosial, pemahaman mereka terhadap ancaman siber sering kali masih terbatas. Banyak siswa yang belum menyadari potensi bahaya seperti *phishing*, pencurian identitas, dan *malware*. Penelitian oleh Veronika Asri Tandirerung et al. (2023) menunjukkan bahwa tingkat pemahaman siswa tentang risiko siber masih rendah sehingga mereka rentan terhadap berbagai serangan siber yang dapat merugikan pribadi maupun institusi pendidikan.

2. Penggunaan Media Sosial dan Potensi Risiko

Media sosial menjadi platform yang sangat populer di kalangan siswa, yang dapat meningkatkan kerentanannya terhadap ancaman privasi dan kejahatan siber. Kebiasaan membagikan informasi pribadi tanpa mempertimbangkan konsekuensinya merupakan salah satu contoh perilaku yang sering terjadi. Dinas Komunikasi dan Informatika Kabupaten Ngawi (2023) dan Pakpahan et al. (2021) menyebutkan bahwa banyak siswa yang tidak mengatur privasi dengan baik pada akun media sosial mereka sehingga data pribadi mereka dapat dengan mudah diakses oleh pihak yang tidak bertanggung jawab. Karena itu, pemahaman mengenai pentingnya pengaturan privasi serta upaya melindungi informasi pribadi di dunia digital perlu ditanamkan sejak awal.

3. Pendidikan dan Literasi Keamanan Informasi

Literasi keamanan informasi di kalangan siswa SMA/SMK masih jauh dari cukup. Pendidikan mengenai topik ini di sekolah-sekolah sering kali belum memadai sehingga siswa cenderung memperoleh pengetahuan terkait keamanan siber melalui pengalaman pribadi atau informasi yang mereka dapatkan secara mandiri. Banyak siswa yang mengakses informasi terkait keamanan siber melalui teman sebaya atau melalui sumber di internet tanpa pemahaman yang mendalam. Oleh karena itu, penting untuk mengintegrasikan materi tentang keamanan siber ke dalam kurikulum pendidikan agar siswa memiliki pengetahuan yang lebih baik dan siap menghadapi ancaman siber di dunia maya (Pakpahan et al., 2021).

4. Respons Terhadap Ancaman Keamanan

Siswa SMA/SMK seringkali tidak tahu cara merespons ancaman keamanan secara efektif. Meskipun mereka mungkin dapat mengenali email *phishing*, mereka sering kali tidak tahu cara melindungi diri atau melaporkan insiden tersebut. Hal ini menunjukkan pentingnya edukasi yang lebih mendalam tentang langkah-langkah pencegahan dan respons terhadap ancaman siber. Sekar (2024) menekankan bahwa pengajaran yang lebih intensif tentang cara merespons ancaman siber dapat membantu siswa untuk mengembangkan perilaku keamanan yang lebih baik dan mengurangi potensi kerugian akibat serangan siber.

5. Pentingnya Pendidikan Keamanan Informasi

Pendidikan mengenai keamanan informasi menjadi semakin penting, terutama bagi siswa berusia 15-18 tahun yang merupakan kelompok pengguna aktif di dunia maya. Siswa pada kelompok usia ini sering kali tidak memiliki pengetahuan yang cukup untuk

melindungi diri mereka dari risiko-risiko seperti pencurian identitas dan penipuan *online*. Penelitian menunjukkan bahwa banyak siswa yang menggunakan layanan internet tanpa memahami pentingnya langkah-langkah pengamanan yang diperlukan untuk melindungi data pribadi mereka (Indrayani, 2020; Sekar, 2024). Oleh karena itu, pengajaran mengenai pentingnya keamanan informasi harus menjadi bagian integral dari kurikulum sekolah agar siswa dapat lebih siap menghadapi ancaman yang ada.

6. Program Edukasi dan Pelatihan

Beberapa sekolah telah mengambil langkah-langkah untuk meningkatkan kesadaran siswa mengenai keamanan informasi melalui program edukasi dan pelatihan. Salah satu contoh program yang efektif adalah pelatihan tentang pengamanan data *cyberspace* yang dilaksanakan di SMK Muhammadiyah 2 Mlati. Dalam program ini, siswa diperkenalkan dengan berbagai teknik untuk melindungi data pribadi mereka di dunia maya, termasuk cara mengamankan akun media sosial, pengenalan terhadap *cybercrime*, dan pengaturan privasi pada perangkat yang mereka gunakan (Indrayani, 2020). Selain itu, penting juga untuk memberikan sosialisasi tentang etika digital untuk membentuk perilaku bertanggung jawab di dunia maya, yang sangat diperlukan di era digital ini (Sekar, 2024).

2.4 Perangkat Analisis Data

2.4.1 RStudio

RStudio merupakan bahasa pemrograman dan lingkungan kerja berbasis *open source* yang digunakan untuk komputasi statistik dan pengolahan data, serta memiliki kemampuan kuat dalam menampilkan grafik melalui berbagai paket analisis yang tersedia. Perangkat lunak ini dikembangkan pertama kali pada tahun 1992 di Universitas Auckland, Selandia Baru oleh Ross Ihaka dan Robert Gentleman (Ariyanto & Rachmadiarti, 2022; Yanti, 2021).

Dalam penelitian ini, RStudio dimanfaatkan untuk melakukan uji statistik seperti uji asumsi klasik, serta analisis regresi linier berganda guna melihat pengaruh variabel independen terhadap variabel dependen. Selain itu, RStudio juga mendukung pembuatan visualisasi data seperti grafik, diagram batang, dan kurva yang membantu dalam memahami pola hubungan antarvariabel secara lebih jelas dan informatif.

2.4.2 IBM SPSS Statistics

IBM SPSS Statistics (*Statistical Package for the Social Sciences*) merupakan perangkat lunak pengolah data statistik yang dirancang salah satunya untuk membantu analisis penelitian kuantitatif. SPSS memiliki kemampuan dalam mengelola serta menganalisis data berukuran besar secara efisien. Perangkat lunak ini digunakan untuk menjalankan berbagai teknik

statistik, baik analisis deskriptif yang bertujuan menggambarkan data secara umum, maupun analisis inferensial yang digunakan untuk menguji hipotesis dan menarik kesimpulan terhadap populasi berdasarkan data sampel (Handayani et al., 2023).

Dalam penelitian ini, SPSS digunakan untuk melakukan analisis regresi linier berganda, yaitu metode statistik yang bertujuan untuk mengetahui sejauh mana variabel independen secara bersama-sama maupun parsial memengaruhi variabel dependen. Melalui SPSS, proses perhitungan koefisien regresi, pengujian signifikansi, serta analisis hubungan antarvariabel dapat dilakukan secara lebih akurat dan sistematis, sehingga hasil penelitian menjadi lebih reliabel dan mudah diinterpretasikan.

2.5 Analisis Deskriptif

Teknik analisis deskriptif merupakan metode yang digunakan untuk menggambarkan atau menjelaskan data yang telah dikumpulkan tanpa bermaksud melakukan generalisasi terhadap populasi yang lebih luas. Melalui analisis ini, peneliti dapat memperoleh gambaran awal mengenai karakteristik dari setiap variabel, baik variabel independen maupun dependen. Analisis deskriptif biasanya disajikan dalam bentuk tabel, diagram, atau tabulasi frekuensi, yang menampilkan ukuran-ukuran statistik seperti nilai rata-rata (*mean*), nilai tengah (*median*), nilai maksimum dan minimum, standar deviasi, serta ukuran penyebaran data lainnya seperti kuartil, desil, dan rentang (*range*). Pendekatan ini memberikan pemahaman dasar mengenai distribusi dan kecenderungan data sebelum dilakukan analisis lebih lanjut (Sahir, 2021).

2.6 Asumsi Klasik

Uji asumsi klasik merupakan tahapan penting dalam analisis data kuantitatif untuk memastikan hasil analisis statistik yang valid dan reliabel. Pengujian ini dilakukan untuk memastikan bahwa model regresi memenuhi syarat-syarat statistik dasar sehingga hasil estimasi tidak bias dan dapat dipercaya. Secara umum, asumsi klasik meliputi beberapa aspek berikut (Iba & Wardhana, 2024):

1. Uji Normalitas

   Asumsi normalitas mengharuskan bahwa data dalam model regresi berdistribusi secara normal. Hal ini penting agar hasil pengujian statistik, seperti uji-t dan uji-F, dapat memberikan estimasi yang akurat. Untuk menguji normalitas data, dapat digunakan uji Kolmogorov-Smirnov atau Shapiro-Wilk. Jika data terbukti tidak berdistribusi normal, dapat dilakukan transformasi data agar distribusinya mendekati normal sebelum analisis dilanjutkan.

2. Uji Homogenitas (Kesamaan Varians)

Asumsi ini menekankan bahwa varians antar kelompok data harus bersifat homogen atau seragam. Homogenitas varians diperlukan terutama dalam analisis varian (ANOVA) dan berbagai uji parametrik lainnya. Pengujian homogenitas biasanya dilakukan menggunakan uji Levene atau uji Bartlett. Apabila hasil menunjukkan varians tidak homogen, metode nonparametrik dapat digunakan sebagai alternatif.

3. Uji Independensi

Asumsi independensi menyatakan bahwa setiap observasi dalam data harus bersifat bebas atau tidak saling memengaruhi. Pelanggaran terhadap asumsi ini dapat menyebabkan bias dalam hasil analisis, terutama pada model regresi. Untuk menjaga independensi data, penting memastikan bahwa proses pengambilan sampel dilakukan dengan tepat dan tidak terjadi keterkaitan antar observasi.

4. Uji Linieritas

Asumsi linieritas menekankan bahwa hubungan antara variabel independen dan variabel dependen bersifat linear. Dengan kata lain, perubahan pada variabel bebas akan menyebabkan perubahan yang searah dan proporsional pada variabel terikat. Uji ini penting untuk memastikan bahwa model regresi dapat menggambarkan hubungan kausal yang logis antara variabel-variabel penelitian.

Meskipun demikian, asumsi klasik tidak selalu harus dipenuhi secara mutlak. Dalam beberapa kondisi, pelanggaran asumsi masih dapat ditoleransi, namun hal tersebut dapat memengaruhi ketepatan, keandalan, serta validitas hasil analisis statistik. Selain keempat asumsi di atas, jenis analisis tertentu mungkin memerlukan pengujian asumsi tambahan sesuai dengan karakteristik model yang digunakan (Iba & Wardhana, 2024).

2.7 Regresi Linier Berganda

2.7.1 Konsep Dasar Analisis Regresi Linier Berganda

Analisis regresi linier berganda adalah teknik statistik yang digunakan untuk mempelajari hubungan antara satu variabel terikat (*dependent variable*) dengan dua atau lebih variabel bebas (*independent variables*) (Sudariana & Yoedani, 2021). Tujuan utama dari analisis ini adalah untuk meramalkan nilai variabel terikat berdasarkan nilai-nilai variabel bebas yang lebih dari dua (Sudariana & Yoedani, 2021). Persamaan umum untuk regresi berganda dapat dituliskan sebagai berikut:

$$Yi = a + b_1X_1 + b_2X_2 + \cdots + b_nX_n + e \quad (2.1)$$

Keterangan:

Yi	: Variabel Dependen.
$b_1, b_2, \ldots, b_n$	: Parameter.
a	: Konstanta.
$X_1 + X_2 + \cdots + X_n$	: Variabel independen.
e	: Komponen *error* atau residual.

2.7.2 Interpretasi Hasil Analisis Regresi Linier Berganda

Hasil dari analisis regresi berganda dapat diinterpretasikan dengan cara berikut (Sudariana & Yoedani, 2021).

1. Uji t digunakan untuk mengetahui apakah setiap variabel independen secara individu memiliki pengaruh yang signifikan terhadap variabel dependen.
2. Uji F berfungsi untuk mengukur sejauh mana seluruh variabel independen secara simultan memberikan pengaruh terhadap variabel dependen.
3. Koefisien Determinasi (R^2) digunakan untuk menggambarkan seberapa besar proporsi variasi pada variabel dependen yang dapat dijelaskan oleh variabel-variabel independen dalam model regresi.

2.7.3 Penelitian Terkait Regresi Linier Berganda dalam Konteks Keamanan Informasi

Beberapa penelitian terdahulu yang menggunakan analisis regresi linier berganda dalam bidang keamanan informasi antara lain:

1. Nursiah et al. (2022) menggunakan regresi linier berganda untuk menganalisis pengaruh persepsi kemudahan penggunaan, manfaat, dan keamanan terhadap minat pengguna dalam menggunakan *mobile banking*.
2. Fermayani et al. (2022) menggunakan regresi linier berganda untuk menganalisis variabel pengaruh privasi, keamanan, dan kepercayaan terhadap niat untuk bertransaksi secara *online* di aplikasi *e-commerce*.
3. Cicilia Warayaan (2025) menggunakan analisis regresi linier berganda untuk mengukur *e-filing*, privasi dan keamanan, serta kesadaran wajib pajak berpengaruh positif terhadap kepatuhan wajib pajak.

2.8 Skala Likert

Menurut Sugiyono (2013), skala Likert merupakan instrumen pengukuran yang digunakan untuk menilai sikap, pendapat, dan persepsi individu maupun kelompok terhadap suatu fenomena sosial. Dalam penggunaannya, setiap variabel penelitian terlebih dahulu diuraikan menjadi beberapa indikator yang kemudian dijadikan acuan dalam penyusunan butir-butir pernyataan atau pertanyaan pada instrumen penelitian.

Dalam penelitian yang berfokus pada tingkat kesadaran keamanan siber di kalangan pengguna aktif, penyusunan kuesioner yang tepat sangat penting agar data yang diperoleh bersifat valid dan reliabel. Desain kuesioner disusun berdasarkan pengukuran variabel independen dan dependen yang relevan dengan tujuan penelitian. Data yang diperoleh melalui kuesioner tersebut kemudian dianalisis menggunakan Skala Likert. Skala ini umum digunakan untuk mengukur tingkat persetujuan responden terhadap berbagai pernyataan, dan dalam penelitian ini, bentuk skala Likert yang digunakan ditampilkan pada Tabel 2.1.

Tabel 2. 1 Skala Likert

No	Keterangan	Skor
1	Sangat Setuju	5
2	Setuju	4
3	Netral	3
4	Tidak Setuju	2
5	Sangat Tidak Setuju	1

2.9 Penelitian Terdahulu dan Kesenjangan Penelitian

Tinjauan pustaka dalam penelitian ini mencakup beberapa penelitian terdahulu dan kesenjangan penelitian yang akan dijelaskan pada Tabel 2.2 berikut:

Tabel 2. 2 Hasil Temuan Penelitian Terdahulu

Judul Penelitian	Metode Penelitian	Hasil Penelitian
Model Perilaku Keamanan Siber pada Pengguna Sosial Media pada Masa Pandemi Covid-19 (Aini et al., 2022)	Penelitian ini menerapkan pendekatan kuantitatif dengan desain survei sebagai metode pengumpulan data dari responden. Data yang diperoleh kemudian dianalisis menggunakan teknik statistik regresi untuk menilai hubungan antarvariabel, serta dilengkapi dengan uji validitas melalui Korelasi Pearson dan uji reliabilitas menggunakan *Cronbach's Alpha*.	Hasil penelitian menunjukkan bahwa pengetahuan, persepsi terhadap risiko, dan kesadaran merupakan faktor signifikan yang memengaruhi perilaku keamanan siber. Selain itu, variabel lain seperti frekuensi penggunaan perangkat elektronik, intensitas akses media sosial, dan pengalaman terhadap insiden siber juga berkontribusi terhadap pembentukan perilaku keamanan. Dalam konteks ini, praktik manajemen kata sandi diidentifikasi sebagai aspek krusial yang berperan penting dalam menjaga keamanan siber individu.
Analisis Tingkat Kesadaran Keamanan *Cyber* di Media Sosial Instagram: Studi Kasus pada Siswa SMK Negeri 1 Banyudono (Mahendra et al., 2024)	Penelitian ini menerapkan pendekatan kuantitatif dengan desain survei deskriptif dan eksplanatori yang dianggap sesuai untuk menggambarkan sekaligus menjelaskan fenomena yang menjadi fokus kajian. Subjek penelitian difokuskan pada siswa SMK Negeri 1 Banyudono, dengan metode pengambilan sampel menggunakan teknik *simple random sampling* serta penentuan jumlah sampel mengacu pada rumus Slovin.	Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber di kalangan siswa, khususnya dalam penggunaan platform Instagram, berada pada kategori tertentu dan dipengaruhi oleh faktor-faktor demografis seperti usia, tingkat kelas, dan jurusan. Temuan ini juga mengidentifikasi area spesifik yang masih memerlukan perhatian, seperti praktik penggunaan kata sandi dan pengelolaan privasi, yang mengindikasikan perlunya peningkatan literasi digital di kalangan siswa.
Analisis Tingkat Security Awareness Dalam Password Behavior Mahasiswa (Studi Kasus	Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei yang menganalisis tingkat kesadaran keamanan serta perilaku dalam penggunaan kata sandi	Hasil penelitian menunjukkan bahwa meskipun sebagian besar mahasiswa memiliki pengetahuan yang cukup mengenai prinsip-prinsip keamanan kata sandi, sikap dan perilaku aktual mereka tidak selalu sejalan dengan

Judul Penelitian	Metode Penelitian	Hasil Penelitian
Mahasiswa FEBI UINSU Medan) (Fauzi, 2024)	di kalangan mahasiswa. Analisis data mencakup statistik deskriptif guna menggambarkan tingkat kesadaran dan perilaku yang ditunjukkan responden, pembobotan dan agregasi data berdasarkan indikator Knowledge, Attitude, and Behavior (KAB) untuk menentukan tingkat kesadaran secara keseluruhan, serta analisis korelasi untuk mengidentifikasi hubungan antar dimensi kesadaran.	pengetahuan tersebut. Ditemukan bahwa praktik keamanan dasar seperti membuat kata sandi yang kuat, tidak membagikan kata sandi kepada orang lain, dan secara rutin mengganti kata sandi masih menjadi tantangan yang signifikan. Temuan ini mengindikasikan adanya kesenjangan antara pemahaman teoretis dan penerapan praktis terkait keamanan siber di kalangan mahasiswa.
Model Perilaku Keamanan Siber pada Pengguna Sistem Informasi Kesehatan pada Masa Pandemi Covid-19 (Herlambang et al., 2020)	Penelitian ini mengadopsi pendekatan kuantitatif dengan desain survei, sejalan dengan penelitian-penelitian sebelumnya, untuk memperoleh data dari pengguna sistem informasi kesehatan. Data yang terkumpul kemudian dianalisis menggunakan metode statistik regresi, dan dalam beberapa kondisi, pendekatan Structural Equation Modeling (SEM) digunakan untuk menguji model perilaku yang diajukan secara lebih menyeluruh.	Secara umum, hasil penelitian menunjukkan bahwa faktor-faktor seperti tingkat kesadaran, pelatihan keamanan, penerapan sanksi, dan persepsi terhadap risiko memiliki pengaruh signifikan terhadap kepatuhan pengguna terhadap kebijakan keamanan informasi. Studi ini menekankan bahwa perilaku keamanan siber memegang peranan penting dalam menjaga kerahasiaan dan integritas data sensitif pasien. Dalam konteks ini, kekuatan dan pengelolaan kata sandi diidentifikasi sebagai elemen krusial dalam mendukung keamanan sistem informasi kesehatan secara keseluruhan.
Factors Affecting Cybersecurity Awareness among University Students (Alqahtani, 2022)	Metode penelitian yang digunakan dalam studi ini adalah pendekatan kuantitatif dengan desain survei. Data dikumpulkan dari 450 mahasiswa universitas melalui kuesioner yang difokuskan pada tiga aspek	Hasil penelitian menunjukkan bahwa seluruh variabel independen—keamanan kata sandi, keamanan peramban, dan aktivitas media sosial—memiliki pengaruh yang signifikan terhadap kesadaran keamanan siber. Namun demikian, temuan juga mengungkap bahwa kesadaran

Judul Penelitian	Metode Penelitian	Hasil Penelitian
	utama, yaitu keamanan kata sandi, keamanan peramban, dan aktivitas media sosial. Analisis data dilakukan secara komprehensif untuk mengevaluasi pengaruh ketiga variabel tersebut terhadap tingkat kesadaran keamanan siber mahasiswa.	praktis mahasiswa, khususnya dalam aspek keamanan kata sandi, masih tergolong rendah. Hal ini tercermin dari perilaku yang kurang ideal, seperti tidak melakukan perubahan kata sandi secara berkala, penggunaan kata sandi yang sama untuk berbagai akun, serta persepsi bahwa kata sandi yang panjang dianggap tidak praktis, meskipun mereka enggan untuk membagikan kata sandi kepada pihak lain.

Meskipun telah terdapat banyak penelitian mengenai perilaku keamanan kata sandi, analisis menunjukkan beberapa kesenjangan penting yang perlu diperhatikan:

1. Kesenjangan Populasi dan Konteks Geografis Spesifik

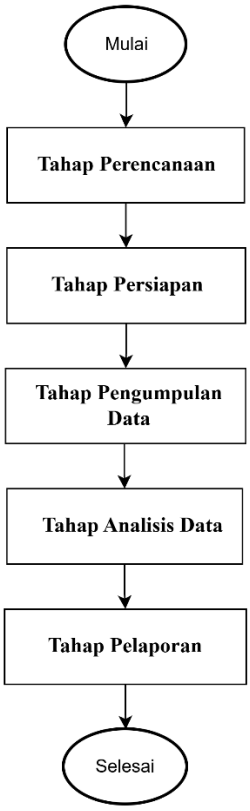
   Beberapa studi sebelumnya, seperti "*Analisis Tingkat Kesadaran Keamanan Siber di Media Sosial Instagram: Studi Kasus pada Siswa SMK Negeri 1 Banyudono*" (Mahendra et al., 2024), telah meneliti kesadaran keamanan siber pada siswa di salah satu SMK yang berada di Indonesia. Namun, fokus utama studi tersebut adalah pada kesadaran siber secara umum, bukan secara spesifik pada perilaku keamanan kata sandi. Di sisi lain, studi-studi yang secara eksplisit meneliti perilaku kata sandi seperti "*Analisis Tingkat Security Awareness dalam Password Behavior Mahasiswa*" (Fauzi, 2024) dan "*Factors Affecting Cybersecurity Awareness among University Students*" (Alqahtani, 2022) lebih banyak menyasar populasi mahasiswa. Hal ini menimbulkan kesenjangan karena perilaku, pemahaman, dan faktor pendorong terkait keamanan siber dapat sangat berbeda antara kelompok usia dan jenjang pendidikan, serta dipengaruhi oleh konteks budaya dan geografis. Oleh karena itu, penelitian yang secara khusus berfokus pada perilaku keamanan kata sandi di kalangan siswa SMA/SMK di Provinsi DIY akan mengisi kekosongan literatur tersebut.

2. Kesenjangan antara Pengetahuan dan Praktik dalam Perilaku Kata Sandi

   Beberapa literatur, termasuk "*Factors Affecting Cybersecurity Awareness among University Students*" (Alqahtani, 2022) dan "*Analisis Tingkat Security Awareness dalam Password Behavior Mahasiswa*" (Fauzi, 2024), secara konsisten menunjukkan adanya kesenjangan antara tingkat pengetahuan atau kesadaran dengan praktik nyata terkait keamanan kata sandi. Meskipun mahasiswa mengetahui pentingnya penggunaan kata sandi yang kuat, dalam praktiknya mereka sering kali enggan untuk mengganti kata sandi secara berkala, menggunakan kata sandi yang sama untuk beberapa akun, atau menghindari penggunaan kata sandi panjang karena dianggap tidak praktis. Penelitian ini bertujuan untuk mengeksplorasi lebih dalam yang menyebabkan terjadinya kesenjangan tersebut pada kalangan siswa SMA/SMK di Provinsi DIY.

BAB III
METODOLOGI PENELITIAN

Metodologi penelitian merupakan pendekatan ilmiah yang digunakan dalam proses penyelidikan untuk memahami dan memecahkan suatu permasalahan secara sistematis. Dalam penelitian ini, metodologi berfungsi sebagai pedoman dalam mengumpulkan, mengolah, serta menganalisis data agar diperoleh hasil yang objektif dan dapat dipertanggungjawabkan. Melalui langkah-langkah yang terstruktur, metodologi penelitian membantu memastikan bahwa proses penelitian berjalan secara cermat, teliti, dan sesuai dengan kaidah ilmiah sehingga hasil yang diperoleh dapat memberikan pengetahuan yang berguna dan relevan dengan tujuan penelitian (Sahir, 2021). Metodologi penelitian ini dapat digambarkan dalam diagram alur pada Gambar 3.1.



Gambar 3. 1 Diagram Alur Penelitian

Berdasarkan alur diagram yang ditampilkan pada Gambar 3.1, dapat dipahami bahwa penelitian ini dilaksanakan melalui beberapa tahapan sebagai berikut:

a. Tahap Perencanaan

Tahap ini berfokus pada pembentukan kerangka logis dan desain penelitian.

1. Metode dan Pendekatan Penelitian: Penentuan penggunaan Metode Penelitian Kuantitatif dan jenis penelitian Eksplanatori untuk menguji hubungan sebab-akibat antarvariabe.
2. Populasi dan Sampel: Penetapan populasi target (siswa SMA/SMK DIY) dan perhitungan ukuran sampel minimal sebanyak 100 responden menggunakan Rumus Slovin.
3. Variabel dan Hipotesis: Identifikasi variabel independen (X1, X2, X3, X4) dan variabel dependen (Y), serta perumusan dugaan sementara mengenai pengaruh positif atau negatif antar variabel (H1 sampai H4).

b. Tahap Persiapan

Tahap ini meliputi penyelesaian aspek teknis dan logistik penelitian sebelum pengumpulan data.

1. Instrumen Penelitian: Penyusunan kuesioner terstruktur dengan Skala Likert lima poin untuk mengukur 5 variabel penelitian.
2. Validasi Instrumen Penelitian: Pelaksanaan uji coba instrumen untuk memastikan terpenuhinya kriteria Validitas (r-hitung > r-tabel) dan Reliabilitas (alpha > 0,7).
3. Teknik Penentuan Sampel: Penentuan metode pengambilan sampel *Stratified Random Sampling* untuk menjamin keterwakilan heterogenitas populasi.
4. Alat Analisis Data: Penetapan penggunaan IBM SPSS Statistics 31 dan RStudio sebagai perangkat lunak utama untuk pengolahan dan analisis data.

c. Tahap Pengumpulan Data

Tahap ini merupakan implementasi lapangan untuk memperoleh data dari subjek penelitian.

1. Metode Pengumpulan Data: Implementasi teknik pengumpulan data menggunakan kuesioner luring dan daring melalui platform *Google Form* untuk efisiensi dan aksesibilitas.
2. Lokasi dan Waktu Penelitian: Pelaksanaan pengumpulan data dilakukan di Provinsi DIY sesuai jadwal yang telah ditentukan, yaitu pada Mei 2025.

d. Tahap Analisis Data

Tahap ini melibatkan pemrosesan dan pengujian data untuk penarikan kesimpulan statistik.

1. Analisis Deskriptif: Penyajian statistik dasar untuk menggambarkan karakteristik responden (asal sekolah, usia, jenis kelamin, tingkat kelas.) dan tingkat kesadaran keamanan kata sandi.
2. Uji Asumsi Klasik: Pengujian prasyarat yang harus dipenuhi oleh model regresi linier berganda, meliputi Uji Normalitas, Uji Linearitas, Uji Multikolinearitas, dan Uji Heteroskedastisitas.
3. Uji Analisis Data: Pengujian hipotesis melalui Analisis Regresi Linier Berganda, termasuk:
    - Uji F (Simultan): Menguji pengaruh seluruh variabel bebas secara kolektif.
    - Uji t (Parsial): Menguji pengaruh masing-masing variabel bebas secara individual.
    - Koefisien Determinasi (R^2): Mengukur proporsi variasi variabel dependen yang dijelaskan oleh variabel independen.

e. Tahap Pelaporan

Tahap ini merupakan tahap akhir dari siklus penelitian, di mana hasil diinterpretasikan dan disusun menjadi kesimpulan.

1. Penarikan Kesimpulan: Interpretasi hasil Uji Analisis Data untuk menentukan penerimaan atau penolakan hipotesis, yang akan menjawab rumusan masalah penelitian.
2. Merumuskan Saran yang relevan bagi pihak-pihak terkait.
3. Menyelesaikan laporan akhir sesuai panduan penulisan institusi.
4. Menyelesaikan seluruh dokumen laporan penelitian secara utuh.

3.1 Metode Penelitian

Metode penelitian kuantitatif merupakan pendekatan yang bersifat sistematis dan digunakan untuk menyelesaikan permasalahan penelitian melalui pengumpulan data yang bersifat terukur serta dapat diolah secara statistik. Pada penelitian ini, data diperoleh menggunakan instrumen yang telah dirancang sebelumnya, kemudian dianalisis dengan metode statistik yang sesuai, dan hasil analisis tersebut menjadi dasar dalam penarikan kesimpulan (Sugiyono, 2013). Proses penelitian kuantitatif membutuhkan perencanaan yang cermat dan penerapan prosedur yang terstruktur agar hasil yang diperoleh dapat diandalkan dan dapat diuji kembali (Sugiyono, 2013).

3.2 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian *explanatory*. Pendekatan tersebut dipilih karena sesuai dengan tujuan penelitian, yaitu untuk menjelaskan hubungan sebab-akibat antarvariabel melalui pengujian hipotesis, sebagaimana dilakukan dalam penelitian oleh Iqbal et al. (2024).

Penggunaan metode kuantitatif memungkinkan pengukuran variabel-variabel penelitian dalam bentuk angka yang kemudian dianalisis menggunakan metode statistik. Pendekatan ini sangat relevan untuk penelitian di bidang keamanan siber, terutama dalam mengukur perilaku dan sikap pengguna secara objektif (Doria, 2024). Selain itu, pendekatan kuantitatif mendukung tujuan penelitian untuk menganalisis faktor-faktor yang memengaruhi perilaku keamanan kata sandi.

3.3 Populasi dan Sampel

3.3.1 Populasi

Menurut Sugiyono (2013), populasi merupakan area generalisasi yang mencakup objek atau subjek dengan karakteristik tertentu yang telah ditentukan untuk diteliti dan dijadikan dasar dalam penarikan kesimpulan. Pengertian ini menegaskan bahwa populasi tidak hanya terbatas pada sekumpulan individu, tetapi juga mencakup keseluruhan kelompok atau wilayah yang menjadi acuan dalam melakukan generalisasi hasil penelitian.

Berdasarkan pengertian tersebut, populasi dalam penelitian ini mencakup seluruh siswa SMA/SMK yang berada di wilayah Provinsi DIY. Populasi ini tergolong dalam kategori populasi terbatas (*finite population*) karena jumlah anggotanya diketahui secara pasti, yaitu sebanyak 152.620 siswa berdasarkan data yang tersedia (Kementerian Pendidikan Dasar dan Menengah, 2025).

Populasi yang digunakan dalam penelitian ini juga bersifat heterogen, karena terdiri dari berbagai jenis sekolah (SMA dan SMK) serta perbedaan status kelembagaan (Negeri dan Swasta). Keberagaman ini menciptakan subkelompok atau strata yang memiliki potensi perbedaan karakteristik, termasuk dalam aspek perilaku keamanan kata sandi. Dalam penelitian sosial yang melibatkan manusia dan fenomena sosial, keberagaman seperti ini memerlukan penentuan batas-batas populasi secara jelas, baik dari segi kuantitatif maupun kualitatif.

3.3.2 Sampel

Sampel merupakan bagian dari populasi yang diambil untuk mewakili keseluruhan populasi dalam suatu penelitian. Menurut Sugiyono (2013), sampel merupakan sebagian dari jumlah serta karakteristik yang dimiliki oleh populasi. Pengertian ini menegaskan bahwa

sampel bukan sekadar bagian acak dari populasi, melainkan harus mencerminkan ciri-ciri utama populasi secara keseluruhan agar kesimpulan yang dihasilkan valid dan dapat digeneralisasikan.

Dalam penelitian kuantitatif, terutama ketika populasi berjumlah besar sehingga tidak memungkinkan untuk meneliti seluruh anggotanya, penentuan ukuran sampel menjadi hal yang krusial. Salah satu metode yang sering digunakan adalah rumus Slovin, yaitu formula yang berfungsi untuk menentukan jumlah minimal sampel yang dibutuhkan ketika ukuran populasi diketahui, tetapi tingkat variasi data dalam populasi belum sepenuhnya diketahui (Antoro, 2024).

Penggunaan rumus Slovin sangat relevan dalam konteks penelitian ini, mengingat jumlah siswa SMA/SMK di Provinsi DIY yang sangat besar. Dalam kondisi seperti ini, pendekatan sensus tidak memungkinkan dilakukan karena keterbatasan waktu, tenaga, dan sumber daya. Oleh karena itu, penentuan sampel dengan rumus Slovin menjadi solusi yang efektif untuk memperoleh data yang representatif dan mendukung validitas temuan penelitian.

Dengan mempertimbangkan tingkat kesalahan (*margin error*) sebesar 10% dan tingkat kepercayaan sebesar 90%, jumlah sampel dalam penelitian ini ditentukan menggunakan pendekatan yang sesuai untuk populasi besar (Mariani, 2018; Sedgwick, 2014), jumlah sampel ditetapkan dengan menggunakan rumus Solvin pada persamaan 3.1 yaitu:

$$n = \frac{N}{1 + N(e)^2} \tag{3.1}$$

Keterangan:

n = ukuran sampel

N = 152.620 (jumlah populasi)

e = *margin error* (10% atau 0.10)

$$n = \frac{152.620}{1 + 152.620 \cdot (0{,}10)^2}$$

$$n = \frac{152.620}{1 + 152.620 \cdot 0{,}01}$$

$$n = \frac{152.620}{1 + 1.526{,}2}$$

$$n = \frac{152.620}{1.527{,}2}$$

$$n = 99{,}93 \text{ (dibulatkan menjadi 100 responden)}$$

Ukuran sampel yang dibutuhkan untuk penelitian ini adalah sekitar 100 responden siswa SMA dan SMK di wilayah Provinsi Daerah Istimewa Yogyakarta (DIY).

Mengacu pada tingkat heterogenitas populasi tersebut, penggunaan teknik *simple random sampling* tidak dianggap cukup representatif karena tidak menjamin keterwakilan setiap subkelompok dalam populasi. Oleh karena itu, metode *stratified random sampling* dipilih sebagai pendekatan pengambilan sampel. Teknik ini memungkinkan setiap strata berdasarkan jenis dan status sekolah terwakili secara proporsional dalam sampel sehingga meningkatkan validitas dan kemampuan generalisasi temuan penelitian terhadap keseluruhan populasi yang beragam (Singh & Mangat, 1996).

3.4 Teknik Penentuan Sampel

Untuk memastikan bahwa data yang dikumpulkan dalam penelitian ini bersifat representatif dan dapat digeneralisasikan untuk seluruh populasi siswa SMA/SMK sederajat di Provinsi DIY, digunakan teknik *Stratified Random Sampling* (sampel acak berstrata) dengan alokasi proporsional (Singh & Mangat, 1996). Teknik ini dipilih secara strategis karena populasi siswa di Provinsi DIY memiliki karakteristik yang heterogen, terutama ditinjau dari jenis sekolah (SMA dan SMK) serta status sekolah (Negeri dan Swasta). Perbedaan-perbedaan karakteristik ini diperkirakan dapat memengaruhi perilaku keamanan kata sandi sehingga pembagian populasi menjadi beberapa strata yang lebih homogen menjadi langkah penting untuk meningkatkan validitas hasil penelitian.

Proses stratifikasi dimulai dengan mengidentifikasi strata yang relevan berdasarkan kombinasi jenis dan status sekolah, yaitu:

1. Siswa SMA Negeri
2. Siswa SMA Swasta
3. Siswa SMK Negeri
4. Siswa SMK Swasta

Setelah strata ditentukan, langkah selanjutnya adalah memperoleh data jumlah siswa dari masing-masing strata secara akurat melalui sumber data resmi dan terbaru, seperti Data Pokok Pendidikan (Dapodik). Informasi ini diperlukan untuk menghitung proporsi alokasi sampel pada masing-masing strata.

Pada kategori sekolah swasta, penelitian secara khusus memilih sekolah yang berada di bawah naungan Muhammadiyah, yaitu SMA Muhammadiyah 1 Prambanan dan SMK Muhammadiyah 1 Wates. Pemilihan ini didasarkan pada pertimbangan konsistensi standar pendidikan dan tata kelola yang terstruktur, sehingga mengurangi potensi bias terkait variasi kualitas manajemen sekolah swasta secara acak. Selain itu, sebagai salah satu lembaga pendidikan terbesar di Indonesia, sekolah Muhammadiyah dinilai cukup representatif untuk menggambarkan kondisi mayoritas sekolah swasta di wilayah DIY.

Ukuran total sampel telah ditentukan sebelumnya menggunakan rumus Slovin dengan *margin of error* sebesar 10%, menghasilkan jumlah sampel sebanyak 100 siswa. Sampel ini kemudian dialokasikan secara proporsional sesuai dengan persentase representasi masing-masing strata dalam populasi. Misalnya, jika siswa SMA Negeri mencakup 25% dari total populasi, maka 25% dari 100 responden (yakni 25 siswa) akan diambil dari strata tersebut.

Pemilihan lokasi sekolah dilakukan dengan mempertimbangkan karakteristik wilayah agar representasi data menjadi lebih komprehensif. SMK Negeri 6 Yogyakarta dipilih untuk mewakili lingkungan perkotaan dengan akses infrastruktur digital yang lebih baik, sedangkan SMA Negeri 2 Wonosari dipilih untuk merepresentasikan wilayah Kabupaten Gunungkidul. Penempatan sampel di luar pusat kota bertujuan untuk menangkap variasi perilaku keamanan siber siswa di wilayah yang lebih terpencil (*remote area*), sehingga temuan tidak hanya menggambarkan kondisi siswa perkotaan.

Setelah proporsi sampel ditetapkan, tahap terakhir adalah pelaksanaan *simple random sampling* di dalam masing-masing strata. Pemilihan responden dilakukan secara acak menggunakan daftar nama yang disediakan oleh sekolah, dengan bantuan metode *random number generator*. Pendekatan ini memastikan bahwa setiap siswa memiliki peluang yang sama untuk terpilih, sehingga meminimalkan bias dan meningkatkan validitas eksternal penelitian. Dengan demikian, hasil yang diperoleh diharapkan mampu menggambarkan kondisi populasi secara lebih akurat dan dapat digeneralisasikan.

3.5 Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini berupa kuesioner terstruktur yang disusun menggunakan *Google Form* untuk mempermudah proses pengumpulan dan pengolahan data (Habagat & Hermosa, 2024). Kuesioner terdiri atas dua bagian utama. Bagian pertama berisi informasi mengenai karakteristik demografis responden, meliputi jenis kelamin, tingkat kelas, usia, dan jenis sekolah. Bagian kedua berisi pernyataan tertutup yang disusun menggunakan skala Likert lima poin, dengan rentang jawaban dari Sangat Tidak Setuju hingga Sangat Setuju.

Kuesioner ini mengukur lima variabel penelitian, yaitu Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, Persepsi Risiko, dan Perilaku Keamanan Kata Sandi, dengan total 28 item pernyataan yang ditampilkan pada Tabel 3.1. Bentuk lengkap kuesioner dapat dilihat pada LAMPIRAN A, sedangkan indikator setiap variabel beserta sumber penyusunannya disajikan dalam LAMPIRAN B. Untuk meningkatkan validitas instrumen dan meminimalkan potensi bias respons, disertakan dua pernyataan negatif yang disebar secara acak di antara pernyataan positif, yaitu PR1 pada variabel Persepsi Risiko dan PKKS6 pada variabel Perilaku Keamanan Kata Sandi.

Seperti yang ditampilkan pada Tabel 3.2 , pernyataan positif diberi skor secara berurutan dari 1 (Sangat Tidak Setuju) hingga 5 (Sangat Setuju), sedangkan pernyataan negatif menggunakan *reverse scoring*, yaitu dari 5 (Sangat Tidak Setuju) hingga 1 (Sangat Setuju), agar hasil interpretasi tetap konsisten. Sebelum kuesioner digunakan dalam pengumpulan data utama, dilakukan uji validitas dan reliabilitas terlebih dahulu untuk memastikan bahwa setiap item pernyataan mampu mengukur variabel yang diteliti secara akurat dan konsisten.

Tabel 3. 1 Operasionalisasi Variabel Penelitian

Variabel	**Kode**	**Pernyataan**	**Jenis**
Kecemasan Ingatan	KI1	Saya merasa tertekan atau stres ketika harus mengingat banyak kata sandi.	Positif
	KI2	Saya lebih mudah mengingat kata sandi yang memiliki arti khusus bagi saya (seperti tanggal lahir atau nama panggilan).	Positif
	KI3	Saya yakin dapat mengingat kata sandi yang saya buat tanpa perlu menuliskannya.	Positif
	KI4	Seiring bertambahnya usia, saya merasa lebih sulit mengingat kata sandi yang kompleks.	Positif
	KI5	Saya khawatir lupa kata sandi lama saat membuat kata sandi baru.	Positif
Pengaruh Teman Sebaya	PTS1	Saya akan merasa malu jika teman-teman tahu akun media sosial saya diretas.	Positif
	PTS2	Teman-teman akan menganggap saya ceroboh jika akun saya diretas.	Positif

	PTS3	Saya khawatir akan menjadi bahan pembicaraan teman-teman jika akun saya diretas.	Positif
	PTS4	Saya terpengaruh untuk memperbarui perangkat lunak karena teman-teman saya melakukannya.	Positif
	PTS5	Saya termotivasi mencadangkan data penting karena melihat teman-teman melakukannya.	Positif
	PTS6	Saya mengikuti kebijakan keamanan sekolah karena teman-teman saya juga mematuhinya.	Positif
Pengalaman Keamanan Siber Pribadi	PKSP1	Saya rutin memeriksa pengaturan privasi di akun media sosial saya.	Positif
	PKSP2	Saya selalu memastikan *anti-virus* di perangkat saya terbaru.	Positif
	PKSP3	Saya segera waspada jika perangkat saya berperilaku tidak normal.	Positif
	PKSP4	Saya menghindari membuka email dari pengirim tidak dikenal.	Positif
	PKSP5	Saya tidak pernah membagikan informasi pribadi di media sosial.	Positif
	PKSP6	Saya berhati-hati dengan tautan pendek yang tidak jelas di media sosial.	Positif
Persepsi Risiko	PR1	Saya merasa akun saya aman dan tidak mungkin diretas.	Negatif
	PR2	Saya khawatir data pembayaran *game online* saya bisa dicuri.	Positif
	PR3	Saya sadar perangkat saya bisa terinfeksi *malware* saat bermain *game online*.	Positif
	PR4	Saya khawatir transaksi *online* saya tidak aman.	Positif
	PR5	Saya menyadari risiko terpengaruh berita palsu di media sosial.	Positif

Perilaku Keamanan Kata Sandi	PKKS1	Saya menggunakan kata sandi yang berbeda untuk akun sekolah dan media sosial.	Positif
	PKKS2	Saya tidak pernah membagi kata sandi akun sekolah dengan teman.	Positif
	PKKS3	Saya menggunakan kombinasi huruf, angka, dan simbol dalam kata sandi.	Positif
	PKKS4	Saya selalu mengunci perangkat saya saat meninggalkannya.	Positif
	PKKS5	Saya selalu menghindari mengklik tautan mencurigakan dalam email.	Positif
	PKKS6	Saya sering mengklik tautan yang ada di email yang dikirim oleh orang yang tidak saya kenal.	Negatif

Tabel 3. 2 Skala Likert untuk Penyataan Positif dan Negatif

Pilihan Jawaban	Skor Pernyataan Positif	Skor Pernyataan Negatif
Sangat Tidak Setuju (STS)	1	5
Tidak Setuju (TS)	2	4
Netral (N)	3	3
Setuju (S)	4	2
Sangat Setuju (SS)	5	1

3.6 Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di Provinsi DIY dengan populasi sasaran siswa SMA dan SMK. Pemilihan lokasi ini didasarkan pada beberapa pertimbangan strategis. Pertama, wilayah ini memiliki keragaman karakteristik siswa dari berbagai latar belakang sosial-ekonomi sehingga memungkinkan pengambilan sampel yang representatif. Kedua, aksesibilitas yang baik dalam menjangkau responden mendukung pelaksanaan penelitian secara efisien dan efektif. Penelitian dilaksanakan selama periode tiga bulan, dimulai dari April hingga September 2025, dengan rincian jadwal sebagai berikut:

1. April 2025: Tahap persiapan penelitian yang meliputi penyusunan dan validasi instrumen penelitian, serta pengurusan perizinan dengan pihak-pihak terkait.

2. Mei 2025: Tahap pengumpulan data dilakukan melalui penyebaran kuesioner online kepada responden yang telah ditentukan. Bukti penyebaran dan pelaksanaan pengumpulan data disertakan pada LAMPIRAN C sebagai dokumentasi pendukung penelitian.
3. Juni - September 2025: Tahap pengolahan dan analisis data, termasuk validasi data, analisis statistik, dan interpretasi hasil penelitian.

3.7 Variabel Penelitian

Variabel penelitian merujuk pada sejumlah faktor yang ditetapkan untuk dianalisis dalam suatu studi guna mengumpulkan data yang relevan. Data ini kemudian menjadi dasar untuk menarik kesimpulan. Dalam penelitian ini, digunakan dua kategori variabel, yaitu variabel dependen (terikat) dan variabel independen (bebas). Penjelasan mengenai masing-masing jenis variabel disajikan sebagai berikut.

3.7.1 Variabel Independen (X)

a. Kecemasan Ingatan (*Memory Anxiety*)

Faktor ini merujuk pada kekhawatiran pengguna mengenai kemampuan mereka untuk mengingat kata sandi yang digunakan, terutama ketika jumlah akun *online* semakin meningkat. Penelitian oleh Ayyagari et al. (2020) menunjukkan bahwa kecemasan ini dapat menghambat penggunaan manajer kata sandi yang seharusnya dapat membantu pengguna mengelola kata sandi mereka dengan lebih aman dan efisien. Selain itu, penelitian lain oleh Grawemeyer & Johnson (2011) juga menunjukkan bahwa kecemasan terhadap memori menjadi alasan utama bagi banyak pengguna untuk menggunakan atau mengelola beberapa kata sandi secara tidak aman. Ketika kata sandi tidak mudah diingat, pengguna sering kali memilih kata sandi yang lemah atau menggunakan strategi yang tidak aman, seperti menulis kata sandi di tempat yang mudah diakses.

b. Pengaruh Teman Sebaya (*Peer Influence*)

Penelitian yang dilakukan oleh Mwagwabi & Hee Jiow (2021) menunjukkan bahwa keberadaan teman sebaya dapat memengaruhi proses pengambilan keputusan individu terkait keamanan kata sandi, yang mengindikasikan bahwa dinamika sosial memiliki peran penting dalam membentuk perilaku keamanan. Selain itu, penelitian yang dilakukan oleh Dupuis & Khan (2018) mengungkapkan bahwa umpan balik dari teman sebaya dapat mendorong pembuatan kata sandi yang lebih kuat dibandingkan dengan penggunaan meteran kata sandi tradisional. Namun, pengaruh teman sebaya juga dapat menghambat kepatuhan remaja terhadap pedoman keamanan kata sandi, sementara norma pribadi cenderung mendorong mereka untuk lebih mematuhi pedoman tersebut.

c. Pengalaman Keamanan Siber Pribadi (*Personal Cybersecurity Experience*)

Pengalaman Pribadi dalam Keamanan Siber merupakan salah satu variabel penting yang secara signifikan memengaruhi perilaku keamanan kata sandi individu (Tan et al., 2024). Pengalaman ini berperan melalui berbagai mekanisme psikologis, seperti peningkatan persepsi terhadap risiko ancaman, sebagaimana dijelaskan dalam Teori Motivasi Proteksi, pembentukan sikap dan norma subjektif dalam Teori Perilaku Terencana, serta penguatan efikasi diri berdasarkan Teori Kognitif Sosial (Zou et al., 2024). Pengalaman langsung terhadap insiden keamanan siber, seperti akun diretas atau informasi pribadi disalahgunakan, sering kali menjadi pemicu yang kuat bagi individu untuk meningkatkan kewaspadaan dan mulai menerapkan praktik keamanan yang lebih baik, termasuk dalam pengelolaan kata sandi (Anwar et al., 2017).

d. Persepsi Risiko (*Perceived Risk*)

Persepsi risiko berhubungan dengan cara individu menilai potensi ancaman yang dapat muncul akibat penggunaan kata sandi yang kurang aman. Penelitian oleh Anwar et al. (2017) menunjukkan bahwa tingkat persepsi risiko yang tinggi dapat mendorong seseorang untuk lebih waspada dalam membuat kata sandi yang kuat serta menghindari perilaku yang berisiko.

Pemilihan keempat variabel independen dalam penelitian ini didasarkan pada tinjauan literatur terdahulu yang disesuaikan dengan karakteristik psikologis remaja dan konteks keamanan siber. Variabel Kecemasan Ingatan dipilih karena beban kognitif terbukti menjadi hambatan utama pengguna dalam membuat kata sandi yang kompleks, sebagaimana temuan Grawemeyer & Johnson (2011). Selanjutnya, variabel Pengaruh Teman Sebaya diangkat mengingat fase perkembangan remaja sangat dipengaruhi oleh validasi sosial, di mana tekanan lingkungan pertemanan sering kali lebih dominan daripada aturan formal. Variabel Pengalaman Keamanan Siber Pribadi disertakan dengan landasan *Protection Motivation Theory* (PMT), yang menyatakan bahwa pengalaman langsung terhadap insiden siber memicu perubahan perilaku yang lebih efektif dibandingkan sekadar pengetahuan teoretis. Terakhir, variabel Persepsi Risiko dipilih sebagai prasyarat dasar kesadaran, karena perilaku keamanan yang protektif tidak akan terbentuk jika individu tidak menyadari adanya ancaman nyata di balik aktivitas digital mereka.

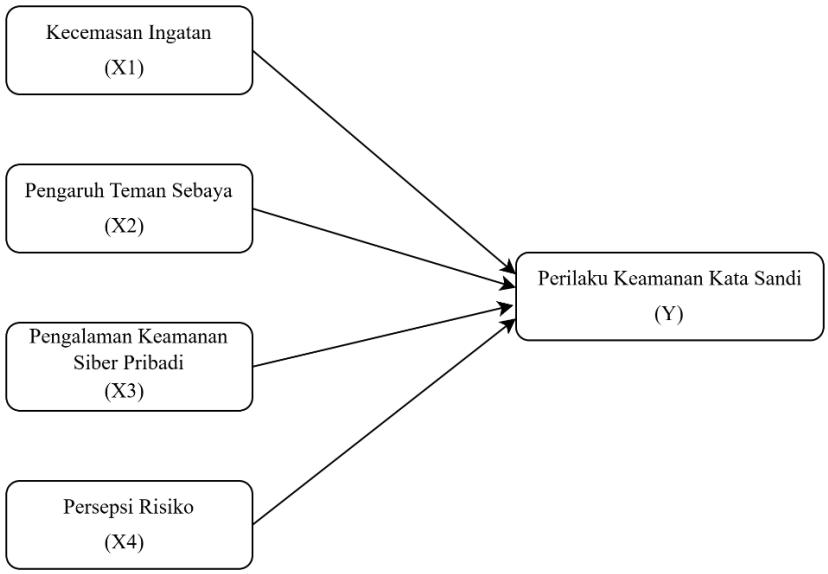
3.7.2 Variabel Dependen (Y)

Variabel dependen dari penelitian ini adalah perilaku keamanan kata sandi. Perilaku Keamanan Kata Sandi merupakan representasi dari tindakan dan kebiasaan individu dalam mengelola serta menggunakan kata sandi untuk menjaga keamanan akun digital mereka. Variabel ini berperan penting dalam konteks keamanan siber, baik pada tingkat individu

maupun organisasi, karena kata sandi umumnya menjadi lapisan pertahanan awal terhadap upaya akses yang tidak sah. Tingkat keamanan yang diterapkan dalam penggunaan kata sandi, seperti kompleksitas, frekuensi penggantian, dan kerahasiaan, mencerminkan sejauh mana individu menerapkan prinsip-prinsip keamanan informasi secara praktis dalam kehidupan sehari-hari.

3.7.3 Kerangka Hubungan Antarvariabel

Pada Gambar 3.2 ditampilkan kerangka hubungan antarvariabel yang menunjukkan arah dan bentuk hubungan yang akan diuji antara variabel-variabel penelitian.



Gambar 3. 2 Hubungan Antarvariabel

3.8 Hipotesis Penelitian

a. Kecemasan Ingatan (*Memory Anxiety*) dan Perilaku Keamanan Kata Sandi

Kecemasan ingatan (*memory anxiety*) berpengaruh signifikan terhadap perilaku keamanan siswa SMA/SMK, terutama dalam pengelolaan kata sandi. Beban kognitif yang tinggi akibat keharusan mengingat berbagai kata sandi mendorong pengguna untuk menerapkan strategi yang kurang aman. Penelitian mengungkapkan bahwa individu cenderung menggunakan kembali kata sandi, menuliskannya, atau membagikannya dengan orang lain sebagai respons terhadap beban ingatan tersebut. Hal ini menunjukkan bahwa kecemasan ingatan memengaruhi pendekatan yang dipilih pengguna dalam mengelola kata sandi mereka (Grawemeyer & Johnson, 2011).

Kecemasan ingatan secara langsung mendorong kecenderungan untuk menggunakan kembali kata sandi. Pengguna sering kali memilih untuk menggunakan kata sandi yang sama atau hanya memodifikasi kata sandi sebelumnya untuk mengurangi beban kognitif yang

diperlukan dalam mempelajari kata sandi baru. Studi menunjukkan bahwa 80% partisipan menggunakan kembali kata sandi mereka di berbagai platform (Grawemeyer & Johnson, 2011). Temuan ini diperkuat oleh fakta bahwa pengguna cenderung mengelompokkan akun mereka dengan kata sandi yang sama alih-alih membuat kata sandi baru (Grawemeyer & Johnson, 2011).

Meskipun alat seperti pengelola kata sandi (*password manager*) dapat mengurangi beban ingatan dan meningkatkan keamanan, kecemasan ingatan yang tinggi sering kali menyebabkan keengganan untuk mengadopsi alat tersebut. Penelitian menyebutkan bahwa ketidakpercayaan terhadap pengelola kata sandi dapat mengurangi daya tarik fitur kemudahan penggunaannya. Keengganan ini juga dipicu oleh ketidaknyamanan pengguna untuk menyerahkan kontrol kata sandi kepada aplikasi. Selain itu, beberapa studi menemukan bahwa pengguna menganggap kemudahan penggunaan sebagai indikasi potensi kelemahan keamanan, sehingga menurunkan kepercayaan terhadap alat tersebut. Dengan demikian, kecemasan ingatan berkontribusi besar terhadap perilaku keamanan yang kurang optimal (Ayyagari et al., 2020).

H1: Kecemasan memori memiliki pengaruh negatif terhadap perilaku keamanan kata sandi.

b. Teman Sebaya (*Peer Influence*) dan Perilaku Keamanan Kata Sandi

Pengaruh teman sebaya memainkan peran krusial dalam membentuk perilaku keamanan siber remaja, khususnya dalam praktik pengelolaan kata sandi. Penelitian menunjukkan bahwa remaja cenderung lebih peka terhadap penilaian teman sebaya dibandingkan ancaman keamanan siber. Pengaruh teman sebaya, yang didefinisikan sebagai kekhawatiran remaja akan ejekan atau gosip dari teman-teman mereka jika akun mereka diretas, berdampak negatif secara signifikan terhadap niat mereka untuk mematuhi pedoman keamanan (Mwagwabi & Hee Jiow, 2021).

Penelitian dari Mwagwabi & Hee Jiow (2021) secara spesifik menemukan bahwa tekanan teman sebaya berdampak negatif pada niat remaja untuk mengikuti pedoman kata sandi di platform media sosial. Dengan kata lain, semakin besar tekanan sosial, seperti ketakutan diejek akibat peretasan, semakin rendah kemungkinan remaja untuk mematuhi rekomendasi keamanan. Temuan ini konsisten dengan penelitian lain yang mengindikasikan bahwa risiko dan sensitivitas terhadap evaluasi teman sebaya meningkat pada usia 13 hingga 16 tahun, yang dapat mendorong perilaku berisiko.

Menariknya, berbeda dengan orang dewasa, remaja tidak termotivasi untuk mematuhi pedoman keamanan hanya karena merasa rentan atau takut terhadap ancaman siber. Sebaliknya, motivasi mereka lebih dipengaruhi oleh rasa malu atau bersalah yang terkait dengan norma sosial dan pribadi. Hasil ini menunjukkan bahwa ketakutan akan penilaian negatif dari teman sebaya memiliki pengaruh lebih besar dalam menghambat kepatuhan terhadap keamanan dibandingkan ketakutan akan ancaman siber itu sendiri. Oleh karena itu, ancaman sosial tampaknya lebih dominan bagi remaja dibandingkan ancaman teknis (Dupuis & Khan, 2018).

H2: Pengaruh teman sebaya berpengaruh positif terhadap perilaku keamanan kata sandi.

c. Pengalaman Keamanan Siber Pribadi (*Personal Cybersecurity Experience*) dan Perilaku Keamanan Kata Sandi

Pengalaman langsung terkait insiden keamanan siber berperan penting dalam membentuk kesadaran dan perilaku keamanan individu. Penelitian oleh Saleh et al. (2025) menunjukkan bahwa pengalaman pribadi maupun keluarga yang pernah mengalami insiden keamanan dapat memicu peningkatan kewaspadaan dan kesadaran terhadap pentingnya menjaga keamanan digital. Hal serupa juga ditemukan oleh Adewusi et al. (2024), yang menjelaskan bahwa pengalaman negatif atau keterlibatan langsung dengan ancaman siber mendorong individu untuk lebih protektif dan aktif mencari informasi keamanan, terutama setelah mengalami pelanggaran data. Secara teoretis, hal ini sejalan dengan Model *Protection Motivation Theory* (PMT) yang dikemukakan oleh Pickering & Taylor (2025), di mana pengalaman pribadi berfungsi sebagai sumber informasi internal yang memengaruhi proses penilaian ancaman (*threat appraisal*) dan penilaian penanggulangan (*coping appraisal*), sehingga membentuk niat serta perilaku keamanan yang lebih baik.

H3: Pengalaman terhadap keamanan siber pribadi berpengaruh positif terhadap perilaku keamanan kata sandi.

d. Persepsi Risiko (*Perceived risk*) dan Perilaku Keamanan Kata Sandi

Penelitian yang dilakukan oleh Zwilling et al. (2022) menegaskan bahwa faktor perilaku manusia memiliki peran penting dalam menjaga keamanan siber. Sementara itu, Kim & Kang (2008) menemukan bahwa tingkat kesadaran individu terhadap risiko berpengaruh terhadap perilaku keamanan kata sandi yang diterapkan. Semakin tinggi persepsi seseorang terhadap risiko keamanan, semakin besar pula kecenderungannya untuk menggunakan kata sandi yang kuat dan aman. Dalam konteks siswa SMA/SMK yang merupakan generasi digital native,

pemahaman terhadap risiko keamanan siber menjadi aspek penting yang dapat mendorong terbentuknya perilaku keamanan kata sandi yang lebih baik.

H4: Persepsi risiko berpengaruh positif terhadap perilaku keamanan kata sandi.

3.9 Metode Pengumpulan Data

Metode pengumpulan data adalah tahapan penting dalam penelitian yang berperan dalam memperoleh informasi yang dibutuhkan untuk mencapai tujuan penelitian. Pada penelitian ini, teknik yang digunakan adalah pengumpulan data melalui kuesioner *online* secara luring dan daring. Penggunaan kuesioner dipilih karena dinilai mampu menjangkau responden secara luas dan efisien, serta memberikan kemudahan dalam proses data (Habagat & Hermosa, 2024). Selain itu, penggunaan platform *online* seperti *Google Forms* memungkinkan pengumpulan data yang cepat dan mudah, serta meminimalkan kesalahan dalam pencatatan data.

3.10 Alat Analisis Data

Dalam penelitian ini digunakan dua perangkat lunak, yaitu RStudio Build 496 dan IBM SPSS Statistics versi 31. Keduanya digunakan untuk analisis deskriptif, uji asumsi klasik, serta regresi linier berganda. Penggunaan dua alat ini dipilih karena RStudio unggul dalam fleksibilitas analisis dan visualisasi, sedangkan SPSS lebih efisien dalam menghasilkan output tabel yang siap dipakai, sehingga analisis dapat dilakukan secara lebih komprehensif dan akurat.

3.10.1 RStudio

Dalam penelitian ini, RStudio digunakan sebagai alat bantu utama untuk memastikan keakuratan hasil dan konsistensi antarperangkat lunak. RStudio digunakan untuk melakukan uji validitas, reliabilitas, serta uji asumsi klasik seperti uji normalitas (Kolmogorov-Smirnov), uji linearitas, uji multikolinearitas, uji heteroskedastisitas (Breusch-Pagan), serta menampilkan hasil dalam bentuk visualisasi grafik *scatterplot*. Seluruh kode program yang digunakan dalam proses analisis tersebut disertakan secara lengkap dalam LAMPIRAN D.

3.10.2 IBM SPSS Statistics 31

Selain RStudio, penelitian ini juga menggunakan IBM SPSS Statistics 31 sebagai alat analisis pendukung dalam melakukan analisis data, khususnya untuk pengujian validitas, reliabilitas, asumsi klasik, serta analisis regresi linier berganda. SPSS dipilih karena kemampuannya dalam mengolah data secara cepat, akurat, dan mudah diinterpretasikan melalui output statistik yang lengkap.

3.11 Validasi Instrumen Penelitian

Validasi instrumen penelitian merupakan tahap krusial yang bertujuan memastikan bahwa alat ukur yang digunakan benar-benar mampu mengukur apa yang dimaksud secara akurat dan konsisten. Sebelum kuesioner disebarkan ke sampel utama, dilakukan uji coba instrumen (*pilot study*) kepada 30 responden yang memiliki karakteristik serupa dengan populasi penelitian namun di luar sampel utama. Penggunaan sampel awal sebanyak 30 responden ini didasarkan pada prinsip distribusi normal atau *Central Limit Theorem*, yang menyatakan bahwa ukuran sampel di atas 30 dianggap memadai untuk mendekati kurva normal guna keperluan uji validitas dan reliabilitas awal instrumen penelitian (Bujang et al., 2024; Kwak & Kim, 2017). Dalam penelitian ini, dua aspek utama yang diperiksa meliputi validitas serta reliabilitas dari instrumen yang digunakan.

a. Uji Validitas

Uji ini dilakukan untuk menilai sejauh mana instrumen penelitian benar-benar mengukur konstruk yang ingin diteliti. Hasil pengujian menghasilkan nilai koefisien korelasi yang mencerminkan kekuatan hubungan antara setiap item pada kuesioner dengan konstruk yang diukur. Suatu item dinyatakan valid apabila nilai r-hitung lebih besar dari r-tabel dan tingkat signifikansinya $\alpha < 0{,}05$. Metode ini digunakan untuk memastikan bahwa setiap butir pertanyaan dalam kuesioner relevan serta mampu menggambarkan variabel yang diteliti secara akurat dan konsisten (Aulia et al., 2023).

b. Uji Reliabilitas

Bertujuan untuk menilai tingkat konsistensi internal dari instrumen penelitian. Teknik yang digunakan yaitu Cronbach’s Alpha, yang dikenal sebagai salah satu metode paling umum dalam menguji reliabilitas suatu kuesioner. Kriteria yang digunakan adalah $\alpha > 0.7$, di mana nilai ini menunjukkan bahwa instrumen memiliki tingkat konsistensi internal yang baik (Aulia et al., 2023). Interpretasi dari nilai Cronbach's Alpha adalah sebagai berikut:

1. $0.7 \leq \alpha < 0.8$: *Acceptable*
2. $0.8 \leq \alpha < 0.9$: *Good*
3. $\alpha \geq 0.9$: *Excellent*

Penggunaan Cronbach's Alpha sangat penting dalam konteks penelitian ini karena indikator ini memberikan gambaran yang jelas tentang sejauh mana item-item dalam kuesioner saling berkorelasi dan mendukung pengukuran konstruk yang sama. Dengan memastikan reliabilitas yang tinggi, data yang dikumpulkan dari kuesioner dapat dipastikan konsisten dan dapat dipercaya.

3.12 Analisis Deskriptif

Analisis deskriptif dalam penelitian ini digunakan untuk memberikan gambaran umum mengenai karakteristik responden serta tingkat kesadaran keamanan kata sandi di kalangan siswa SMA/SMK sederajat di Provinsi DIY. Analisis ini bertujuan untuk mengidentifikasi pola distribusi data dan memahami karakteristik dasar dari setiap variabel penelitian sebelum dilakukan analisis. Visualisasi data dilakukan menggunakan dua jenis diagram, yaitu diagram *pie* dan diagram batang.

1. Diagram *pie* digunakan untuk merepresentasikan karakteristik responden berdasarkan beberapa kategori, yaitu:
   a. Asal sekolah
   b. Jenis kelamin
   c. Usia
   d. Tingkat kelas
2. Diagram batang digunakan untuk menggambarkan tingkat kesadaran keamanan kata sandi, yang diukur melalui variabel Perilaku Keamanan Kata Sandi (PKKS). Melalui diagram batang, dapat dilihat distribusi rata-rata skor dari setiap indikator yang merepresentasikan perilaku keamanan kata sandi responden.

Dengan demikian, penggunaan diagram *pie* dan diagram batang dalam analisis deskriptif ini mempermudah interpretasi hasil serta memberikan pemahaman visual mengenai profil responden dan kecenderungan perilaku keamanan kata sandi siswa secara keseluruhan.

3.13 Uji Asumsi Klasik

a. Uji Normalitas

Untuk mengetahui apakah data dalam model regresi berdistribusi normal atau tidak. Distribusi normal merupakan salah satu asumsi dasar dalam analisis regresi linier berganda, karena model regresi yang baik mengharuskan nilai residual (kesalahan) menyebar secara normal (Iba & Wardhana, 2024). Apabila data tidak berdistribusi normal, maka hasil estimasi dan pengujian hipotesis dapat menjadi tidak valid. Dalam penelitian ini, uji normalitas dilakukan menggunakan metode Kolmogorov-Smirnov karena jumlah sampel penelitian lebih dari 50 responden (Ghasemi & Zahediasl, 2012; Iba & Wardhana, 2024). Sebagai dasar pengambilan keputusan, kriteria yang digunakan adalah sebagai berikut (Iba & Wardhana, 2024):

1. Data berdistribusi normal apabila nilai Sig. (*p-value*) > 0,05.
2. Data tidak berdistribusi normal apabila nilai Sig. (*p-value*) ≤ 0,05.

b. Uji Linearitas

Uji ini bertujuan untuk menilai apakah terdapat hubungan yang bersifat linear secara signifikan antara dua variabel. Hubungan linear mengindikasikan bahwa setiap perubahan pada variabel independen (X) akan diikuti oleh perubahan yang searah atau proporsional pada variabel dependen (Y). Oleh karena itu, dalam model regresi yang ideal, kedua variabel tersebut diharapkan menunjukkan pola hubungan yang linear. Penentuan hasil uji linearitas pada SPSS didasarkan pada nilai *Deviation from Linearity* (Sig.), dengan kriteria sebagai berikut (Iba & Wardhana, 2024):

1. Jika nilai Sig. > 0,05, maka dapat disimpulkan bahwa terdapat hubungan linear yang signifikan antara variabel independen dan variabel dependen.
2. Sebaliknya, jika nilai Sig. < 0,05, maka dapat disimpulkan bahwa hubungan antara kedua variabel tidak bersifat linear secara signifikan.

Pengujian asumsi linearitas menggunakan RStudio dilakukan melalui analisis visual dengan grafik *scatterplot*. Asumsi linearitas dianggap terpenuhi apabila hasil plot data menunjukkan pola yang jelas, baik dengan arah hubungan positif maupun negatif. Namun, jika titik-titik pada grafik *scatterplot* tidak membentuk pola tertentu atau tampak menyebar secara acak, maka dapat disimpulkan bahwa asumsi linearitas tidak terpenuhi (Iba & Wardhana, 2024).

c. Uji Multikolinearitas

Uji ini digunakan untuk mengidentifikasi apakah terdapat hubungan atau korelasi yang tinggi antar variabel independen dalam model regresi. Model regresi yang ideal seharusnya bebas dari korelasi kuat antar variabel bebas. Deteksi multikolinearitas dilakukan dengan memperhatikan nilai *Tolerance* dan *Variance Inflation Factor* (VIF). Nilai VIF menunjukkan sejauh mana varians dari koefisien regresi meningkat akibat adanya korelasi antar variabel independen. Dasar pengambilan keputusannya adalah sebagai berikut (Sudariana & Yoedani, 2021).

1. Jika nilai *Tolerance* > 0,10 dan VIF < 10, maka model regresi dinyatakan bebas dari masalah multikolinearitas.
2. Sebaliknya, jika nilai *Tolerance* < 0,10 dan VIF > 10, maka model regresi menunjukkan adanya indikasi multikolinearitas antar variabel independen.

d. Uji Heteroskedastisitas

Uji ini bertujuan untuk mendeteksi ada atau tidaknya perbedaan varians residual antar satu pengamatan dengan pengamatan lainnya dalam model regresi. Apabila varians residual antar pengamatan bersifat konstan, kondisi tersebut disebut homoskedastisitas. Sebaliknya, jika varians residual bervariasi, maka disebut heteroskedastisitas. Model regresi yang ideal adalah model yang memenuhi asumsi homoskedastisitas, artinya tidak menunjukkan gejala heteroskedastisitas (Sudariana & Yoedani, 2021).

Dalam penelitian ini, uji heteroskedastisitas dilakukan menggunakan SPSS dengan menganalisis pola sebaran titik pada grafik *scatterplot* antara nilai residual dan nilai prediksi. Dasar penafsirannya sebagai berikut:

a. Jika titik-titik membentuk pola tertentu secara teratur, seperti pola bergelombang atau menyempit dan melebar, maka hal tersebut mengindikasikan adanya gejala heteroskedastisitas (Sudariana & Yoedani, 2021).
b. Namun, jika titik-titik tersebar secara acak di atas dan di bawah sumbu Y tanpa menunjukkan pola tertentu, maka dapat disimpulkan bahwa model regresi tidak mengalami heteroskedastisitas. (Sudariana & Yoedani, 2021).

Selain menggunakan SPSS, pengujian heteroskedastisitas juga dilakukan menggunakan RStudio dengan metode Breusch-Pagan *Test*. Uji ini berfungsi untuk mendeteksi ada atau tidaknya heteroskedastisitas secara statistik dengan melihat nilai *p-value*. Jika nilai *p-value* < 0,05 maka menunjukkan adanya heteroskedastisitas, sedangkan jika *p-value* > 0,05 maka model dianggap bebas dari masalah heteroskedastisitas (Iba & Wardhana, 2024).

3.14 Uji Analisis Data

a. Analisis Regresi Linier Berganda

Analisis regresi linier berganda adalah metode yang digunakan untuk mengaitkan beberapa variabel independen dengan satu variabel dependen. Tujuan dari analisis ini adalah untuk mengetahui arah dan besarnya pengaruh antara variabel independen dan variabel dependen, apakah hubungan tersebut bersifat positif atau negatif (Sudariana & Yoedani, 2021). Rumus yang digunakan untuk pengujian regresi linier berganda adalah sebagai berikut:

$$Y = a + b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 + e \qquad 3.1$$

Keterangan:

Y : Variabel Dependen (Perilaku Keamanan Kata Sandi)

b_1, b_2, b_3, b_4 : Koefisien regresi masing-masing variabel independen.

a : Konstanta.

$X_1 + X_2 + X_3 + X_4$: Variabel independen (Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, Persepsi Risiko)

e : Komponen *error* atau residual.

b. Uji t (Parsial)

Derajat signifikansi yang digunakan dalam uji t adalah 0,10, yang berarti tingkat kepercayaan penelitian sebesar 90%. Jika nilai signifikansi (Sig.) lebih kecil dari 0,10, maka hipotesis alternatif (Ha) diterima. Hal ini menunjukkan bahwa variabel independen memiliki pengaruh secara parsial (individu) terhadap variabel dependen. (Sudariana & Yoedani, 2021).

c. Uji F (Simultan)

Uji F digunakan untuk mengetahui apakah seluruh variabel independen dalam model memiliki pengaruh secara simultan atau bersama-sama terhadap variabel dependen. Pengujian ini dilakukan dengan tingkat signifikansi 0,10, yang berasal dari tingkat kepercayaan sebesar 90%. Apabila nilai signifikansi hasil uji lebih kecil dari batas signifikansi tersebut, maka hipotesis alternatif diterima. Hal ini menunjukkan bahwa variabel independen secara keseluruhan memberikan pengaruh yang signifikan terhadap variabel dependen. (Sudariana & Yoedani, 2021).

d. Analisis Koefisien Determinasi (R^2)

Uji koefisien determinasi (R^2) berfungsi untuk menilai seberapa besar kemampuan variabel independen (X) dalam menjelaskan variasi atau perubahan yang terjadi pada variabel dependen (Y). Nilai R^2 berada dalam kisaran antara 0 hingga 1, di mana $R^2 = 0$ berarti variabel independen sama sekali tidak memengaruhi variabel dependen, sedangkan $R^2 = 1$ menunjukkan bahwa seluruh variasi pada variabel dependen dapat dijelaskan sepenuhnya oleh variabel independen (Sudariana & Yoedani, 2021).

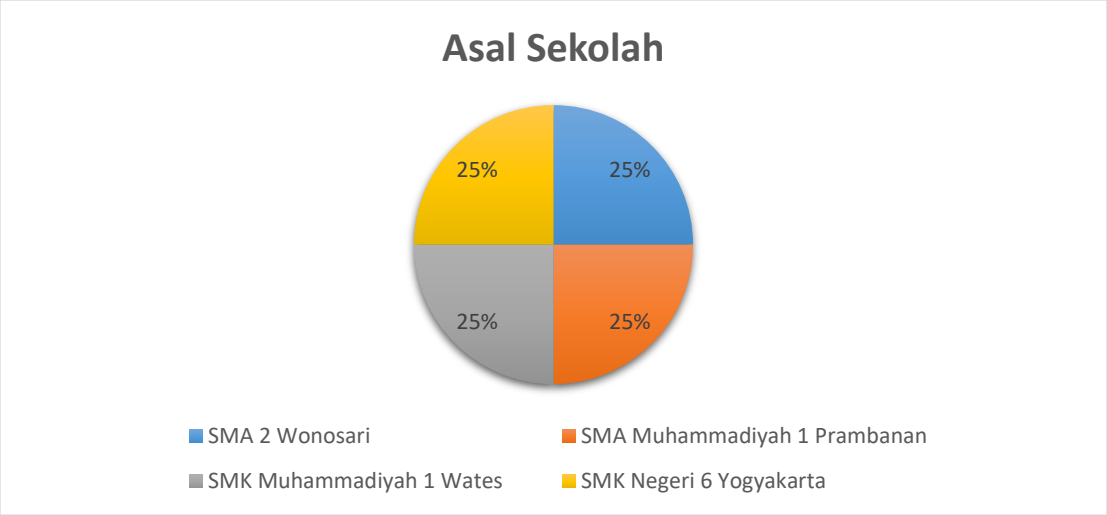
BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Analisis Deskripstif

Penelitian ini melibatkan responden dengan latar belakang demografis dan sosial yang beragam guna memastikan bahwa data yang dikumpulkan mampu merepresentasikan variasi yang ada dalam populasi penelitian. Pada bagian ini, akan disajikan deskripsi data mengenai karakteristik responden penelitian. Responden dalam penelitian ini berjumlah 100 siswa yang berasal dari empat sekolah berbeda di Provinsi DIY.

4.1.1 Karakteristik Responden Berdasarkan Asal Sekolah

Responden penelitian ini berasal dari empat sekolah menengah atas (SMA/SMK) di Provinsi DIY. Distribusi responden dari masing-masing sekolah disajikan secara merata, di mana setiap sekolah diwakili oleh 25 siswa.



Gambar 4. 1 Diagram *Pie* Asal Sekolah

Berdasarkan Gambar 4.1, dapat dilihat bahwa penelitian ini melibatkan partisipasi yang seimbang dari keempat sekolah yang telah ditetapkan sebagai lokasi penelitian, dengan masing-masing menyumbang 25% dari total sampel.

4.1.2 Karakteristik Responden Berdasarkan Jenis Kelamin

Karakteristik responden berdasarkan jenis kelamin bertujuan Puntuk mengidentifikasi proporsi siswa laki-laki dan perempuan yang terlibat dalam penelitian ini.

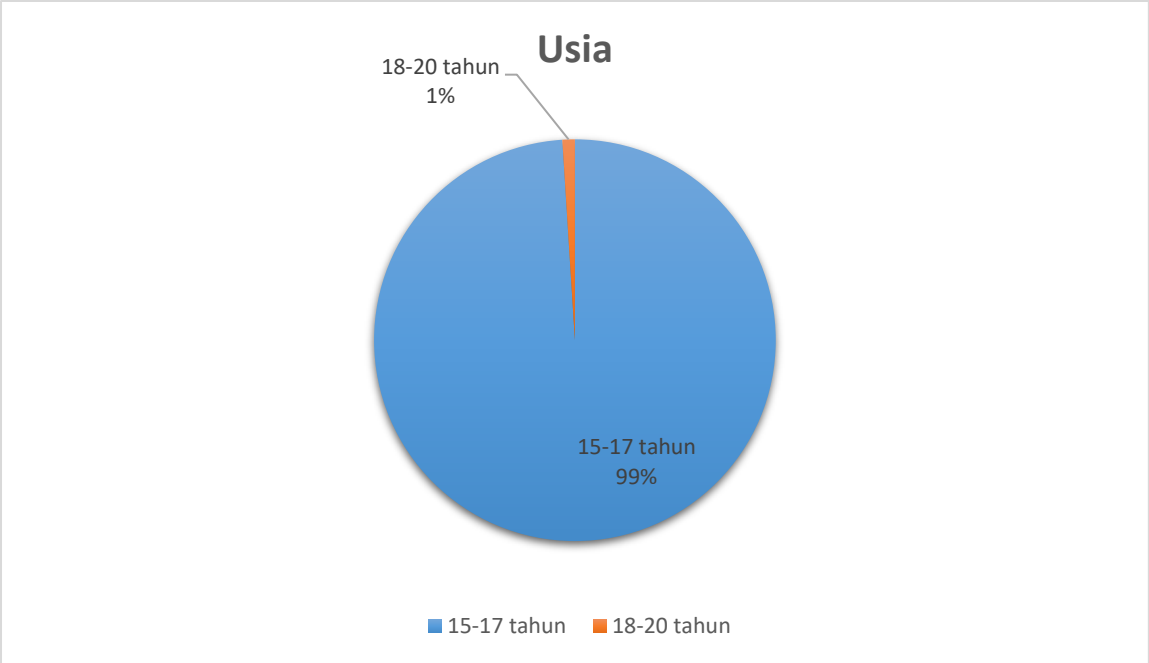


Gambar 4. 2 Diagram *Pie* Jenis Kelamin

Gambar 4.2 menunjukkan bahwa responden dalam penelitian ini didominasi oleh perempuan sebanyak 57 orang (57%), sedangkan responden laki-laki berjumlah 43 orang (43%).

4.1.3 Karakteristik Responden Berdasarkan Usia

Distribusi usia responden dikelompokkan untuk mengetahui rentang usia mayoritas siswa yang menjadi sampel penelitian.

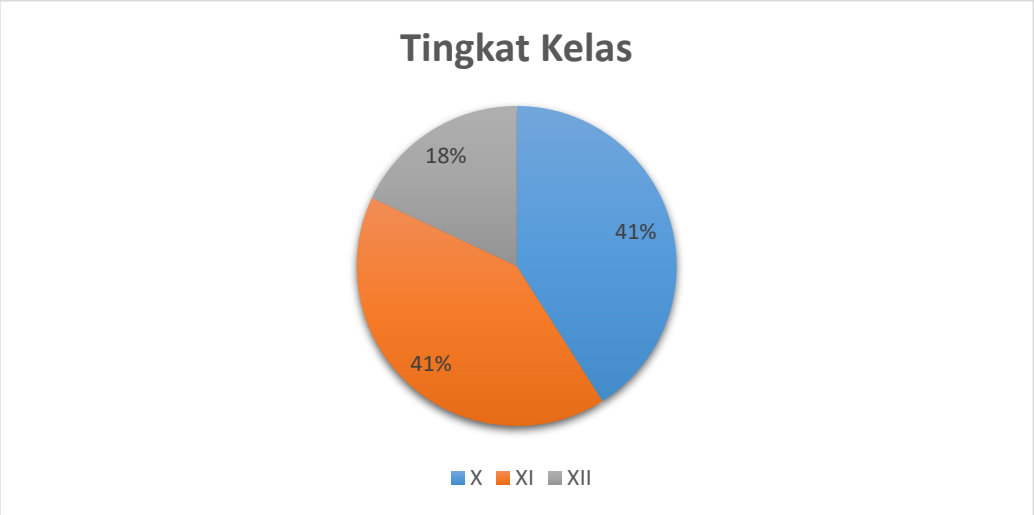


Gambar 4. 3 Diagram *Pie* Usia

Berdasarkan Gambar 4.3, dapat diketahui bahwa mayoritas responden, yaitu sebanyak 99 siswa (99%), berada dalam rentang usia 15-17 tahun, yang merupakan usia tipikal siswa SMA/SMK. Sisanya, sebanyak 1 siswa (1%), berada pada rentang usia 18-20 tahun.

4.1.4 Karakteristik Responden Berdasarkan Tingkat Kelas

Data tingkat kelas responden memberikan gambaran mengenai sebaran partisipasi siswa dari kelas X, XI, dan XII.



Gambar 4. 4 Diagram *Pie* Tingkat Kelas

Dari Gambar 4.4, terlihat bahwa responden dari Kelas X dan Kelas XI memiliki proporsi yang sama besar, masing-masing sebanyak 41 siswa (41%). Sementara itu, responden dari Kelas XII berjumlah 18 siswa (18%). Terdapat 1 responden yang tidak mengisi data tingkat kelas.

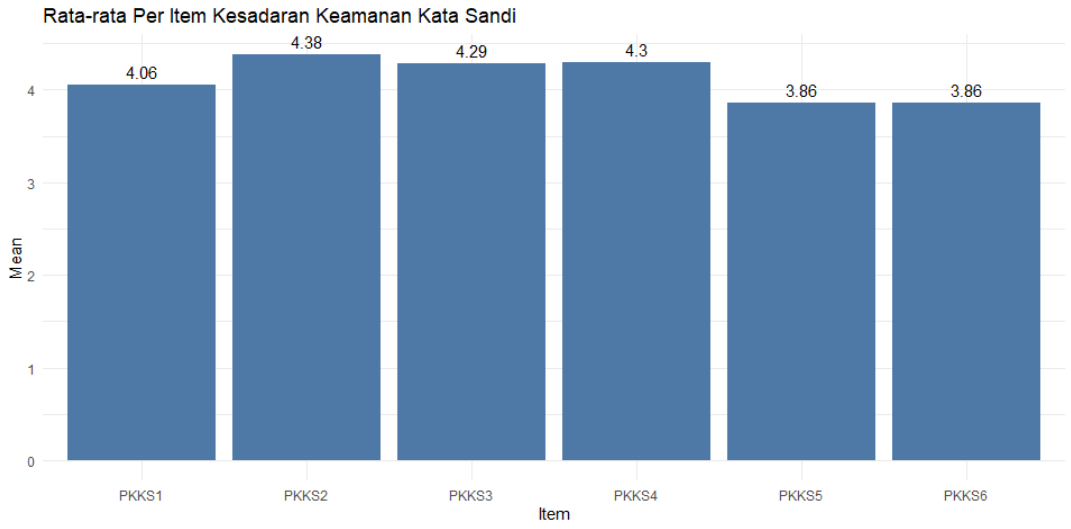
4.1.5 Analisis Tingkat Kesadaran Keamanan Kata Sandi pada Siswa SMA/SMK

Variabel Perilaku Keamanan Kata Sandi diukur melalui enam butir pernyataan (PKKS1–PKKS6) dengan menggunakan skala Likert lima poin, yang berkisar dari 1 = Sangat Rendah/Tidak Pernah hingga 5 = Sangat Tinggi/Selalu. Nilai rata-rata (*mean*) digunakan sebagai indikator untuk menilai tingkat kesadaran siswa terhadap praktik keamanan kata sandi.

	vars	n	mean	sd	median	trimmed	mad	min	max	range	skew	kurtosis	se
PKKS1	1	100	4.06	0.95	4	4.20	1.48	1	5	4	-1.23	1.61	0.10
PKKS2	2	100	4.38	1.01	5	4.62	0.00	1	5	4	-1.96	3.37	0.10
PKKS3	3	100	4.29	0.70	4	4.35	0.00	1	5	4	-1.50	4.79	0.07
PKKS4	4	100	4.30	1.00	5	4.53	0.00	1	5	4	-1.58	1.83	0.10
PKKS5	5	100	3.86	0.93	4	3.98	0.00	1	5	4	-1.13	1.01	0.09
PKKS6	6	100	3.86	1.30	4	4.01	1.48	1	5	4	-0.71	-0.86	0.13

	vars	n	mean	sd	median	trimmed	mad	min	max	range	skew	kurtosis	se
Perilaku_Keamanan_Kata_Sandi	1	100	4.12	0.22	4.17	4.11	0.25	3.67	4.67	1	0.36	-0.14	0.02

Gambar 4. 5 Analisis Deskriptif Variabel Perilaku Keamanan Kata Sandi



Gambar 4. 6 Diagram Batang Rata-rata Variabel Perilaku Kemanana Kata Sandi

Berdasarkan Gambar 4.5 dan Gambar 4.6, dapat dilihat nilai rata-rata (*mean*) dari masing-masing item pernyataan. Hasil dari kedua gambar tersebut kemudian dirangkum dan disajikan secara keseluruhan dalam Tabel 4.1 sebagai dasar untuk penarikan kesimpulan.

Tabel 4. 1 Kesimpulan Hasil Analisis Variabel Perilaku Kemanana Kata Sandi

Kode Soal	**Pertanyaan**	**Mean**	**sd**	**Interpretasi**
PKKS1	Menggunakan kata sandi berbeda untuk akun sekolah dan medsos	4.06	0.95	Baik
PKKS2	Tidak pernah membagi kata sandi akun sekolah dengan teman	4.38	1.01	Sangat Baik
PKKS3	Menggunakan kombinasi huruf, angka, dan simbol dalam kata sandi	4.29	0.70	Sangat Baik
PKKS4	Selalu mengunci perangkat saat meninggalkannya	4.30	1.00	Sangat Baik
PKKS5	Selalu menghindari mengklik tautan mencurigakan dalam email	3.86	0.93	Baik
PKKS6	Sering mengklik tautan di email yang dikirim oleh orang tidak dikenal	3.86	1.30	Baik
Total Rata-Rata	Perilaku Keamanan Kata Sandi	4.12	0.22	Baik

Berdasarkan hasil analisis deskriptif variabel Perilaku Keamanan Kata Sandi (PKKS) pada Tabel 4.1, siswa menunjukkan tingkat kesadaran yang sangat baik pada aspek perilaku dasar dengan rata-rata nilai antara 4,29 hingga 4,38, di mana nilai tertinggi pada PKKS2 (4,38) mencerminkan kesadaran tinggi untuk tidak membagikan kata sandi kepada orang lain. Namun, aspek perilaku yang perlu ditingkatkan tampak pada PKKS5 (menghindari tautan mencurigakan yang dikirim melalui email) dan PKKS1 (penggunaan kata sandi berbeda untuk setiap akun) dengan rata-rata antara 3,86 hingga 4,06, menunjukkan bahwa sebagian siswa belum sepenuhnya konsisten menerapkan praktik keamanan digital secara menyeluruh. Selain itu, meskipun PKKS1 (4,06) masih tergolong tinggi, hasil ini mengindikasikan bahwa siswa lebih fokus pada kekuatan kata sandi secara individual (PKKS3: 4,29) daripada pengelolaan kata sandi antar akun. Nilai terendah pada PKKS5/PKKS6 (3,86) juga menunjukkan bahwa kewaspadaan terhadap tautan mencurigakan yang dikirim melalui email masih rendah dan menjadi aspek yang perlu ditingkatkan dalam upaya memperkuat perilaku keamanan digital siswa SMA/SMK di Provinsi DIY.

4.2 Validasi Intrumen Penelitian

a. Uji Validitas

Uji validitas digunakan untuk memastikan bahwa setiap item dalam instrumen penelitian benar-benar mengukur aspek yang dimaksud. Instrumen dinyatakan valid apabila nilai r hitung > r tabel atau Sig. < 0,05, sedangkan jika r hitung ≤ r tabel atau Sig. > 0,05 maka item dianggap tidak valid.

Correlation matrix

	KI1	KI2	KI3	KI4	KI5	TOTAL KI	PTS1	PTS2	PTS3	PTS4	PTS5	PTS6	TOTAL PTS	PKSP1	PKSP2	PKSP3
KI1	1.00	0.22	0.52	0.39	0.58	0.77	0.22	0.05	0.11	0.06	0.17	0.38	0.24	0.31	0.39	0.34
KI2	0.22	1.00	0.32	0.39	0.41	0.65	0.20	0.35	0.09	0.18	0.31	0.07	0.30	0.34	0.38	0.29
KI3	0.52	0.32	1.00	0.30	0.61	0.77	0.29	0.01	0.00	0.05	0.22	0.42	0.23	0.31	0.41	0.24
KI4	0.39	0.39	0.30	1.00	0.28	0.63	0.21	0.16	-0.04	0.36	0.26	0.15	0.27	0.16	0.12	0.09
KI5	0.58	0.41	0.61	0.28	1.00	0.80	0.31	0.22	0.31	0.11	0.19	0.40	0.38	0.26	0.34	0.23
TOTAL KI	0.77	0.65	0.77	0.63	0.80	1.00	0.33	0.22	0.13	0.20	0.32	0.40	0.39	0.39	0.47	0.34
PTS1	0.22	0.20	0.29	0.21	0.31	0.33	1.00	0.50	0.49	0.38	0.12	0.26	0.72	0.50	0.42	0.23
PTS2	0.05	0.35	0.01	0.16	0.22	0.22	0.50	1.00	0.71	0.37	0.05	0.13	0.72	0.52	0.44	0.41
PTS3	0.11	0.09	0.00	-0.04	0.31	0.13	0.49	0.71	1.00	0.26	0.07	0.24	0.71	0.21	0.24	0.25
PTS4	0.06	0.18	0.05	0.36	0.11	0.20	0.38	0.37	0.26	1.00	0.54	0.32	0.71	0.36	0.36	0.30
PTS5	0.17	0.31	0.22	0.26	0.19	0.32	0.12	0.05	0.07	0.54	1.00	0.56	0.53	0.38	0.42	0.41
PTS6	0.38	0.07	0.42	0.15	0.40	0.40	0.26	0.13	0.24	0.32	0.56	1.00	0.59	0.48	0.42	0.54
TOTAL PTS	0.24	0.30	0.23	0.27	0.38	0.39	0.72	0.72	0.71	0.71	0.53	0.59	1.00	0.61	0.57	0.52
PKSP1	0.31	0.34	0.31	0.16	0.26	0.39	0.50	0.52	0.21	0.36	0.38	0.48	0.61	1.00	0.80	0.76
PKSP2	0.39	0.38	0.41	0.12	0.34	0.47	0.42	0.44	0.24	0.36	0.42	0.42	0.57	0.80	1.00	0.76
PKSP3	0.34	0.29	0.24	0.09	0.23	0.34	0.23	0.41	0.25	0.30	0.41	0.54	0.52	0.76	0.76	1.00
PKSP4	0.39	0.47	0.45	0.05	0.53	0.54	0.46	0.50	0.37	0.29	0.25	0.56	0.61	0.65	0.72	0.72
PKSP5	0.14	0.43	0.20	0.08	0.23	0.31	0.28	0.44	0.30	0.41	0.45	0.50	0.58	0.47	0.72	0.62
PKSP6	0.19	0.33	0.17	-0.03	0.38	0.30	0.37	0.47	0.45	0.38	0.38	0.56	0.64	0.58	0.67	0.81
TOTAL PKSP	0.33	0.43	0.33	0.09	0.37	0.44	0.43	0.54	0.35	0.41	0.45	0.59	0.68	0.82	0.90	0.89
PR1	0.36	0.30	0.14	0.34	0.27	0.39	0.66	0.52	0.52	0.45	0.39	0.31	0.72	0.49	0.39	0.34
PR2	0.24	0.07	-0.08	0.39	0.21	0.22	0.30	0.57	0.46	0.51	0.40	0.25	0.62	0.27	0.31	0.21
PR3	0.14	0.31	0.25	0.24	0.26	0.33	0.27	0.37	0.30	0.61	0.58	0.50	0.64	0.42	0.44	0.37
PR4	0.15	0.46	0.04	0.18	0.30	0.31	0.32	0.48	0.33	0.49	0.57	0.36	0.62	0.45	0.41	0.31
PR5	0.24	0.34	0.13	0.24	0.27	0.34	0.40	0.58	0.42	0.44	0.50	0.48	0.70	0.59	0.50	0.60
TOTAL PR	0.28	0.37	0.11	0.34	0.33	0.39	0.48	0.63	0.50	0.62	0.61	0.47	0.82	0.55	0.51	0.45
PKKS1	0.32	0.15	0.18	0.27	0.18	0.31	0.10	0.22	0.16	0.19	0.17	0.45	0.31	0.27	0.31	0.20
PKKS2	0.04	-0.04	0.02	0.17	0.12	0.08	0.29	0.17	0.19	0.29	0.17	0.36	0.36	0.16	0.21	0.03
PKKS3	0.18	0.03	0.15	0.18	0.21	0.21	0.32	0.28	0.21	0.32	0.31	0.69	0.52	0.42	0.32	0.29
PKKS4	0.42	0.15	0.08	0.45	0.11	0.33	0.32	0.28	0.14	0.33	0.47	0.41	0.47	0.38	0.40	0.34
PKKS5	0.31	0.09	0.07	0.15	0.08	0.20	0.28	-0.04	-0.01	0.20	0.31	0.48	0.28	0.25	0.29	0.17

Gambar 4. 7 Hasil semua Variabel dari Uji Validitas dengan RStudio

Correlations

		KI1	KI2	KI3	KI4	KI5	TOTAL KI
KI1	Pearson Correlation	1	.225	.521**	.387*	.584***	.766***
	Sig. (2-tailed)		.232	.003	.034	<,001	<,001
	N	30	30	30	30	30	30
KI2	Pearson Correlation	.225	1	.318	.393*	.408*	.651***
	Sig. (2-tailed)	.232		.087	.032	.025	<,001
	N	30	30	30	30	30	30
KI3	Pearson Correlation	.521**	.318	1	.305	.609***	.765***
	Sig. (2-tailed)	.003	.087		.102	<,001	<,001
	N	30	30	30	30	30	30
KI4	Pearson Correlation	.387*	.393*	.305	1	.278	.631***
	Sig. (2-tailed)	.034	.032	.102		.137	<,001
	N	30	30	30	30	30	30
KI5	Pearson Correlation	.584***	.408*	.609***	.278	1	.798***
	Sig. (2-tailed)	<,001	.025	<,001	.137		<,001
	N	30	30	30	30	30	30
TOTAL KI	Pearson Correlation	.766***	.651***	.765***	.631***	.798***	1
	Sig. (2-tailed)	<,001	<,001	<,001	<,001	<,001	
	N	30	30	30	30	30	30

Gambar 4. 8 Hasil Uji Validitas Variabel Kecemasan Ingatan dengan SPSS

Correlations

		TOTAL PTS
PTS1	Pearson Correlation	.716***
	Sig. (2-tailed)	<,001
	N	30
PTS2	Pearson Correlation	.725***
	Sig. (2-tailed)	<,001
	N	30
PTS3	Pearson Correlation	.715***
	Sig. (2-tailed)	<,001
	N	30
PTS4	Pearson Correlation	.710***
	Sig. (2-tailed)	<,001
	N	30
PTS5	Pearson Correlation	.532**
	Sig. (2-tailed)	.002
	N	30
PTS6	Pearson Correlation	.595***
	Sig. (2-tailed)	<,001
	N	30
TOTAL PTS	Pearson Correlation	1
	Sig. (2-tailed)	
	N	30

Gambar 4. 9 Hasil Uji Validitas Variabel Pengaruh Teman Sebaya dengan SPSS

Correlations

		TOTAL PKSP
PKSP1	Pearson Correlation	.819***
	Sig. (2-tailed)	<,001
	N	30
PKSP2	Pearson Correlation	.899***
	Sig. (2-tailed)	<,001
	N	30
PKSP3	Pearson Correlation	.890***
	Sig. (2-tailed)	<,001
	N	30
PKSP4	Pearson Correlation	.878***
	Sig. (2-tailed)	<,001
	N	30
PKSP5	Pearson Correlation	.831***
	Sig. (2-tailed)	<,001
	N	30
PKSP6	Pearson Correlation	.891***
	Sig. (2-tailed)	<,001
	N	30
TOTAL PKSP	Pearson Correlation	1
	Sig. (2-tailed)	
	N	30

Gambar 4. 10 Hasil Uji Validitas Variabel Perilaku Keamanan Siber Pribadi dengan SPSS

Correlations

		PR1	PR2	PR3	PR4	PR5	TOTAL PR
PR1	Pearson Correlation	1	.404*	.340	.506**	.566**	.686***
	Sig. (2-tailed)		.027	.066	.004	.001	<,001
	N	30	30	30	30	30	30
PR2	Pearson Correlation	.404*	1	.614***	.634***	.433*	.778***
	Sig. (2-tailed)	.027		<,001	<,001	.017	<,001
	N	30	30	30	30	30	30
PR3	Pearson Correlation	.340	.614***	1	.759***	.533**	.807***
	Sig. (2-tailed)	.066	<,001		<,001	.002	<,001
	N	30	30	30	30	30	30
PR4	Pearson Correlation	.506**	.634***	.759***	1	.709***	.911***
	Sig. (2-tailed)	.004	<,001	<,001		<,001	<,001
	N	30	30	30	30	30	30
PR5	Pearson Correlation	.566**	.433*	.533**	.709***	1	.815***
	Sig. (2-tailed)	.001	.017	.002	<,001		<,001
	N	30	30	30	30	30	30
TOTAL PR	Pearson Correlation	.686***	.778***	.807***	.911***	.815***	1
	Sig. (2-tailed)	<,001	<,001	<,001	<,001	<,001	
	N	30	30	30	30	30	30

Gambar 4. 11 Hasil Uji Validitas Variabel Persepsi Risiko dengan SPSS

Correlations

		TOTAL PKKS
PKKS1	Pearson Correlation	.838***
	Sig. (2-tailed)	<,001
	N	30
PKKS2	Pearson Correlation	.831***
	Sig. (2-tailed)	<,001
	N	30
PKKS3	Pearson Correlation	.848***
	Sig. (2-tailed)	<,001
	N	30
PKKS4	Pearson Correlation	.815***
	Sig. (2-tailed)	<,001
	N	30
PKKS5	Pearson Correlation	.805***
	Sig. (2-tailed)	<,001
	N	30
PKKS6	Pearson Correlation	.806***
	Sig. (2-tailed)	<,001
	N	30
TOTAL PKKS	Pearson Correlation	1
	Sig. (2-tailed)	
	N	30

Gambar 4. 12 Hasil Uji Validitas Variabel Perilaku Keamanan Kata Sandi dengan SPSS

Berdasarkan hasil yang ditampilkan pada Gambar 4.7 yang diuji menggunakan RStudio, serta Gambar 4.8, Gambar 4.9, Gambar 4.10, Gambar 4.11, dan Gambar 4.12 yang diuji menggunakan SPSS, hasil uji validitas dari seluruh variabel penelitian dirangkum secara menyeluruh dalam Tabel 4.2. Tabel 4.2 menjadi dasar dalam penarikan kesimpulan mengenai tingkat validitas setiap item pernyataan pada masing-masing variabel yang digunakan dalam penelitian ini.

Tabel 4. 2 Hasil Kesimpulan Uji Validitas

Variabel	**Item**	**Korelasi Pearson (SPSS & Rstudio)**	**Sig. (2-tailed) (SPSS)**	**Keterangan**
Perilaku Keamanan Kata Sandi (Y1)	PKKS1	0,838	<0,001	Valid
	PKKS2	0,831	<0,001	Valid
	PKKS3	0,848	<0,001	Valid
	PKKS4	0,815	<0,001	Valid
	PKKS5	0,805	<0,001	Valid

	PKKS6	0,806	<0,001	Valid
Kecemasan Ingatan (X1)	KI1	0,766	<0,001	Valid
	KI2	0,651	0,001	Valid
	KI3	0,765	<0,001	Valid
	KI4	0,631	0,001	Valid
	KI5	0,798	<0,001	Valid
Pengaruh Teman Sebaya (X2)	PTS1	0,716	<0,001	Valid
	PTS2	0,725	<0,001	Valid
	PTS3	0,715	<0,001	Valid
	PTS4	0,710	<0,001	Valid
	PTS5	0,532	0,002	Valid
	PTS6	0,595	<0,001	Valid
Pengalaman Keamanan Siber Pribadi (X3)	PKSP1	0,819	<0,001	Valid
	PKSP2	0,899	<0,001	Valid
	PKSP3	0,890	<0,001	Valid
	PKSP4	0,878	<0,001	Valid
	PKSP5	0,831	<0,001	Valid
	PKSP6	0,891	<0,001	Valid
Persepsi Risiko (X4)	PR1	0,686	<0,001	Valid
	PR2	0,778	<0,001	Valid
	PR3	0,807	<0,001	Valid
	PR4	0,911	<0,001	Valid
	PR5	0,815	<0,001	Valid

Berdasarkan Tabel 4.2, dapat disimpulkan bahwa seluruh item kuesioner dinyatakan valid setelah melalui uji validitas menggunakan dua alat analisis, yaitu SPSS dan RStudio, di mana keduanya menghasilkan output yang menunjukkan kesamaan hasil.

b. Uji Reliabilitas

Uji reliabilitas dilakukan untuk memastikan bahwa kuesioner yang digunakan konsisten dan dapat diandalkan. Pengujian menggunakan metode Cronbach's Alpha, dengan kriteria instrumen dianggap reliabel jika nilai Alpha > 0.70.

Kecemasan Ingatan

Cronbach's Alpha	N of Items
.770	5

Pengaruh Teman Sebaya

Cronbach's Alpha	N of Items
.753	6

Pengalaman Keamanan Siber Pribadi

Cronbach's Alpha	N of Items
.928	6

Persepsi Risiko

Cronbach's Alpha	N of Items
.859	5

Perilaku Keamanan Kata Sandi

Cronbach's Alpha	N of Items
.900	6

Gambar 4. 13 Hasil Uji Reliabilitas dengan SPSS

```
Reliability analysis
Call: psych::alpha(x = x1)

  raw_alpha std.alpha G6(smc) average_r S/N   ase mean   sd median_r
      0.77      0.77    0.76       0.4 3.4 0.066  3.4 0.88     0.39

Reliability analysis
Call: psych::alpha(x = x2)

  raw_alpha std.alpha G6(smc) average_r S/N  ase mean   sd median_r
      0.75      0.75     0.8      0.33   3 0.07  3.1 0.82     0.32

Reliability analysis
Call: psych::alpha(x = x3)

  raw_alpha std.alpha G6(smc) average_r S/N   ase mean   sd median_r
      0.93      0.93    0.95       0.7  14 0.021  3.9 0.91     0.72

 Reliability analysis
 Call: psych::alpha(x = x4)

   raw_alpha std.alpha G6(smc) average_r S/N   ase mean sd median_r
       0.86      0.86    0.86      0.55 6.1 0.039  3.3  1     0.55

 Reliability analysis
 Call: psych::alpha(x = y1)

   raw_alpha std.alpha G6(smc) average_r S/N   ase mean  sd median_r
        0.9      0.91    0.91      0.62 9.6 0.028  3.3 1.3     0.61
```

Gambar 4. 14 Hasil Uji Reliabilitas dengan RStudio

Berdasarkan Gambar 4.13 dan Gambar 4.14, hasil uji reliabilitas yang diperoleh dari kedua alat analisis dirangkum secara keseluruhan pada Tabel 4.3 sebagai dasar untuk penarikan kesimpulan mengenai tingkat reliabilitas instrumen penelitian.

Tabel 4. 3 Kesimpulan Uji Reliabilitas

Variabel	Jumlah	Cronbach's Alpha	Keterangan
Kecemasan Ingatan (X1)	5	0.77	*Acceptable*
Pengaruh Teman Sebaya (X2)	6	0.75	*Acceptable*
Pengalaman Keamanan Siber Pribadi (X3)	6	0.93	*Excellent*
Persepsi Risiko (X4)	5	0.86	*Good*
Perilaku Keamanan Kata Sandi (Y)	6	0.9	*Excellent*

Berdasarkan Tabel 4.3, seluruh variabel dinyatakan reliabel karena memiliki nilai Cronbach's Alpha di atas ambang batas 0,70. Meskipun demikian, terdapat perbedaan tingkat konsistensi antarvariabel. Variabel Pengalaman Keamanan Siber Pribadi dan Perilaku Keamanan Kata Sandi menunjukkan nilai Alpha di atas 0,90 yang masuk dalam kategori *Excellent*. Hal ini mengindikasikan konsistensi internal yang sangat tinggi, di mana responden memahami dan menjawab pola pertanyaan pada variabel ini secara sangat seragam. Di sisi lain, variabel Kecemasan Ingatan dan Pengaruh Teman Sebaya berada pada kisaran di atas 0,70 yang masuk kategori *Acceptable*. Perbedaan ini wajar dalam penelitian sosial, di mana nilai tersebut tetap menunjukkan bahwa instrumen valid dan layak digunakan, meskipun variasi jawaban responden pada variabel psikososial (seperti kecemasan dan pengaruh teman) cenderung lebih beragam dibandingkan variabel perilaku teknis. Meskipun pengujian dilakukan menggunakan dua alat analisis, yaitu RStudio dan SPSS, hasil yang diperoleh menunjukkan kesamaan yang konsisten antara keduanya.

4.3 Uji Asumsi Klasik

Uji asumsi klasik dilakukan untuk memastikan bahwa model regresi linier berganda yang dibangun memenuhi persyaratan statistik agar hasil estimasi tidak bias, konsisten, dan efisien (*BLUE - Best Linear Unbiased Estimator*). Uji asumsi klasik yang dilakukan meliputi uji normalitas, uji linearitas, uji multikolinearitas, dan uji heteroskedastisitas.

4.3.1 Uji Normalitas

Uji normalitas bertujuan untuk memeriksa apakah nilai residual model regresi terdistribusi secara normal. Normalitas residual penting untuk validitas inferensi statistik. Dalam penelitian ini, uji normalitas dilakukan menggunakan uji Kolmogorov-Smirnov.

a. Hasil Uji menggunakan SPSS

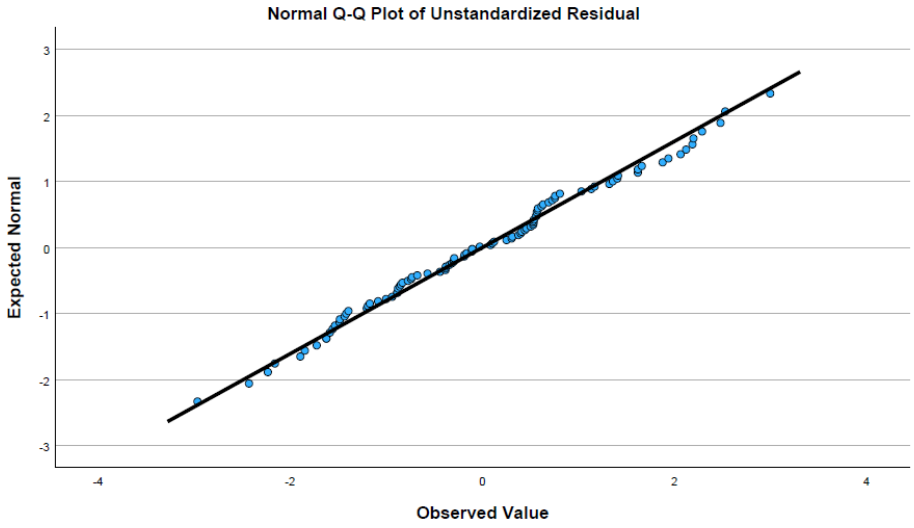
Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Unstandardized Residual	.062	100	.200*	.988	100	.542

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Gambar 4. 15 Hasil Uji Normalitas dengan SPSS



Gambar 4. 16 Grafik Q-Q Residual Plot Uji Normalitas dengan SPSS

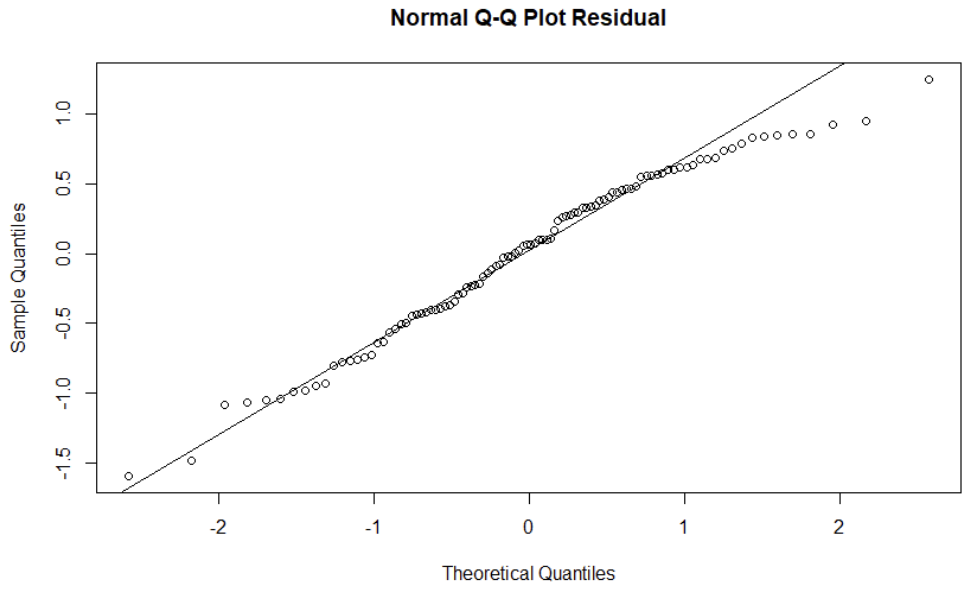
Berdasarkan Gambar 4.15, nilai signifikansi pada uji kolmogorov-smirnov sebesar 0,542, yang jauh lebih besar dari 0,05. Secara visual, Gambar 4.16. juga memperlihatkan histogram residual yang membentuk pola menyerupai kurva normal, serta titik-titik pada grafik Normal Q-Q Plot yang mengikuti garis diagonal.

b. Hasil Uji menggunakan Rstudio

```
        Asymptotic one-sample Kolmogorov-Smirnov test

data:  residuals_std
D = 0.061624, p-value = 0.8421
alternative hypothesis: two-sided
```

Gambar 4. 17 Hasil Uji Normalitas dengan RStudio



Gambar 4. 18 Grafik Q-Q Plot Residual Uji Normalitas dengan RStudio

Berdasarkan Gambar 4.17 yang dihasilkan dari analsis menggunakan RStudio, nilai *p-value* pada uji kolmogorov-smirnov adalah sebesar 0,8421. Karena nilai tersebut lebih besar dari 0,05 (0,8421 > 0,05), maka dapat disimpulkan bahwa residual pada model regresi berdistribusi normal. Dengan demikian, asumsi normalitas residual telah terpenuhi.

Berdasarkan hasil dari kedua alat analisis, nilai signifikansi uji normalitas residual diketahui lebih besar dari 0,05. Hal ini menunjukkan bahwa data residual berdistribusi normal. Visualisasi histogram dan Q-Q Plot pada Gambar 4.16 dan Gambar 4.18 turut memperkuat hasil tersebut, di mana sebaran data tampak mengikuti pola garis diagonal sehingga dapat disimpulkan bahwa asumsi normalitas telah terpenuhi.

4.3.2 Uji Linearitas

Uji linearitas bertujuan untuk mengetahui apakah hubungan antara variabel independen dan variabel dependen bersifat linear.

a. Hasil Uji menggunakan SPSS

Dasar pengambilan keputusan pada uji linearitas menggunakan SPSS dapat ditentukan berdasarkan nilai *Deviation from Linearity* (Sig.).

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
Y1 * X1	Between Groups	(Combined)	8.754	4	2.188	1.316	.270
		Linearity	3.571	1	3.571	2.147	.146
		Deviation from Linearity	5.182	3	1.727	1.039	.379
	Within Groups		157.996	95	1.663		
	Total		166.750	99			

			Sum of Squares	df	Mean Square	F	Sig.
Y1 * X2	Between Groups	(Combined)	13.242	4	3.310	2.049	.094
		Linearity	3.113	1	3.113	1.927	.168
		Deviation from Linearity	10.129	3	3.376	2.089	.107
	Within Groups		153.508	95	1.616		
	Total		166.750	99			

			Sum of Squares	df	Mean Square	F	Sig.
Y1 * X3	Between Groups	(Combined)	17.811	8	2.226	1.360	.225
		Linearity	4.204	1	4.204	2.568	.112
		Deviation from Linearity	13.607	7	1.944	1.188	.318
	Within Groups		148.939	91	1.637		
	Total		166.750	99			

			Sum of Squares	df	Mean Square	F	Sig.
Y1 * X4	Between Groups	(Combined)	9.700	4	2.425	1.467	.218
		Linearity	.327	1	.327	.198	.657
		Deviation from Linearity	9.373	3	3.124	1.890	.137
	Within Groups		157.050	95	1.653		
	Total		166.750	99			

Gambar 4. 19 Uji Linearitas menggunakan SPSS

Dilihat pada Gambar 4.19 dapat disimpulkan pada Tabel 4.4, sebagai berikut:

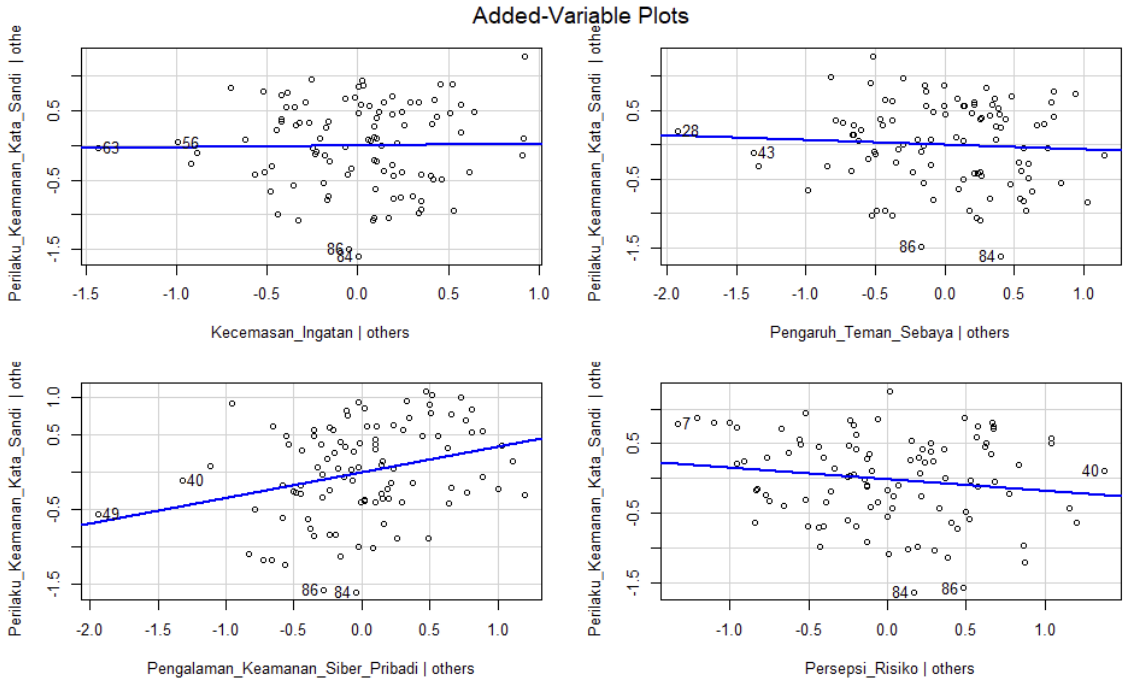
Tabel 4. 4 Kesimpulan Uji Linearitas SPSS

Hubungan	**Variabel independen**	**Nilai Sig. (Deviation from Linearity)**	**Kesimpulan (Sig. > 0,05)**
Y1 * X1	Kecemasan Ingatan	0,379	Linear
Y1 * X2	Pengaruh Teman Sebaya	0,107	Linear
Y1 * X3	Pengalaman Keamanan Siber Pribadi	0,318	Linear
Y1 * X4	Persepsi Risiko	0,137	Linear

Berdasarkan kriteria Sig. > 0,05 pada baris "*Deviation from Linearity*," semua hubungan antara variabel independen (X1, X2, X3, X4) dan variabel dependen (Y1) memenuhi asumsi linearitas (terdapat hubungan linear yang signifikan).

b. Hasil Uji menggunakan RStudio

Uji ini dilakukan secara visual dengan mengamati pola sebaran titik-titik pada grafik partial residual plots untuk setiap variabel independen terhadap variabel dependen. Pada Gambar 4.20 ini, garis biru menunjukkan hubungan linear yang diprediksi oleh model, sedangkan sebaran titik-titik (residual) idealnya tersebar secara acak di sekitar garis tersebut tanpa membentuk pola tertentu.



Gambar 4. 20 Grafik Uji Linearitas menggunakan RStudio

Uji linearitas pada Gambar 4.20 dilakukan secara visual menggunakan *Added-Variable Plots* (plot regresi parsial) yang dihasilkan dari RStudio. Grafik ini memiliki dua elemen utama, yaitu titik-titik data dan garis biru. Titik-titik menunjukkan nilai residual atau penyimpangan data dari setiap responden, sementara angka kecil di dekat titik tertentu menandakan bahwa titik tersebut merupakan outlier. Garis biru adalah garis regresi parsial yang menunjukkan pola hubungan antara variabel. Jika garis ini tampak lurus dan tidak membentuk lengkungan, maka hubungan antarvariabel dapat dianggap linear.

Hasil pengamatan terhadap keempat grafik menunjukkan bahwa variabel Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko semuanya memiliki garis biru yang lurus dan cenderung naik ke arah kanan atas. Hal ini menandakan adanya hubungan yang linear dan positif antara masing-masing variabel independen dengan Perilaku Keamanan Kata Sandi sebagai variabel dependen. Meskipun

terdapat beberapa outlier, pola sebaran titik tetap acak di sekitar garis dan tidak membentuk pola lengkung tertentu, sehingga linearitas secara keseluruhan terpenuhi.

Hasil analisis dari kedua alat, baik melalui Gambr 4.19 pada SPSS maupun Grafik *Scatter Plots* pada RStudio, menunjukkan hasil yang konsisten bahwa seluruh variabel independen (X1, X2, X3, X4) memiliki hubungan linear dengan variabel dependen, yaitu Perilaku Keamanan Kata Sandi.

4.3.3 Uji Multikolinearitas

Uji multikolinearitas dilakukan untuk mengetahui apakah terdapat korelasi yang tinggi atau sempurna antara variabel independen dalam model regresi. Pengujian ini dilakukan dengan memeriksa nilai Variance Inflation Factor (VIF), di mana secara umum nilai VIF < 10 menandakan bahwa tidak terjadi multikolinearitas.

a. Hasil Uji menggunakan SPSS

Model		Collinearity Statistics VIF
1	(Constant)	
	X1	1.022
	X2	1.026
	X3	1.015
	X4	1.029

Gambar 4. 21 Hasil Uji Multikolinearitas dengan SPSS

Berdasarkan Gambar 4.21, nilai VIF (*Variance Inflation Factor*) untuk seluruh variabel independen menunjukkan angka yang sangat kecil, dengan nilai tertinggi sebesar 1,029 pada variabel X4. Karena seluruh nilai VIF berada di bawah 10, maka dapat disimpulkan bahwa tidak terdapat masalah multikolinearitas dalam model regresi.

b. Hasil Uji menggunakan RStudio

```
[1] ">>> Hasil Uji Multikolinearitas (VIF):"
> print(vif(model_revised))
                Kecemasan_Ingatan             Pengaruh_Teman_Sebaya Pengalaman_Keamanan_Siber_Pribadi
                         1.021744                          1.025842                          1.015320
                  Persepsi_Risiko
                         1.028725
```

Gambar 4. 22 Hasil Uji Multikolinearitas dengan RStudio

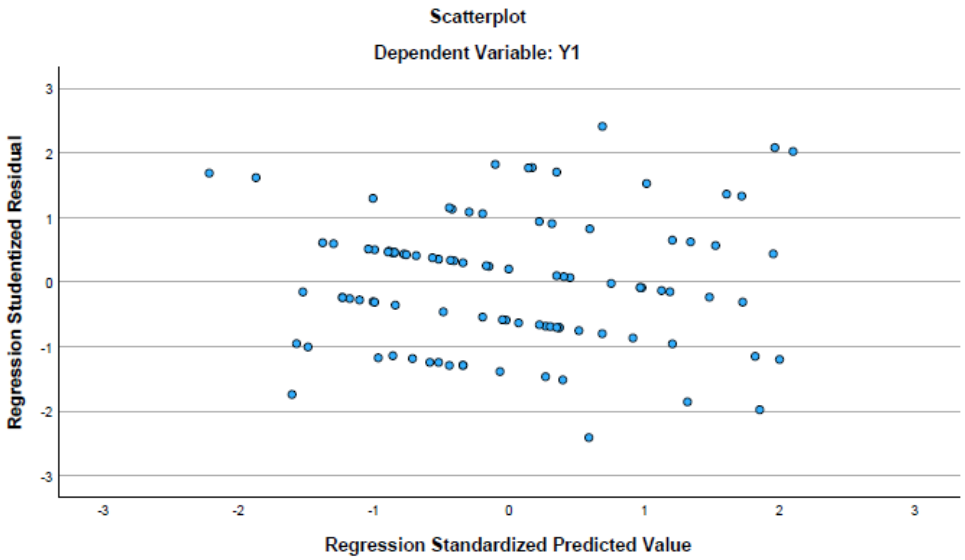
Gambar 4.22 menunjukkan hasil uji multikolinearitas menggunakan RStudio, di mana seluruh variabel independen memiliki nilai VIF (*Variance Inflation Factor*) < 10. Hal ini mengindikasikan bahwa model regresi tidak mengalami masalah multikolinearitas.

Meskipun terdapat sedikit perbedaan pada nilai tertinggi dan nilai masing-masing variabel antara hasil analisis SPSS dan RStudio, secara keseluruhan keduanya menunjukkan hasil yang konsisten, yaitu tidak adanya indikasi multikolinearitas dalam model regresi.

4.3.4 Uji Heteroskedastisitas

Uji heteroskedastisitas dilakukan untuk mengidentifikasi ada atau tidaknya perbedaan varians residual pada berbagai tingkat nilai variabel independen. Kondisi heteroskedastisitas dapat menyebabkan estimasi standar error menjadi tidak akurat. Pada RStudio, pengujian dilakukan menggunakan metode Breusch–Pagan, dengan ketentuan bahwa apabila nilai p-value > α (0,05), maka model dinyatakan bebas dari heteroskedastisitas. Sementara itu, pada SPSS, pengujian dilakukan secara visual melalui *scatterplot* antara nilai *standardized predicted value* dan *studentized residual*. Model dinyatakan tidak mengalami heteroskedastisitas apabila titik-titik pada *scatterplot* menyebar secara acak dan tidak membentuk pola tertentu.

a. Hasil Uji menggunakan SPSS



Gambar 4. 23 Hasil Uji Heteroskedastisitas dengan SPSS

Pengujian heteroskedastisitas dilakukan dengan memeriksa pola penyebaran titik pada Scatterplot antara nilai prediksi (*Regression Standardized Predicted Value*) pada sumbu X dan nilai residual (*Regression Studentized Residual*) pada sumbu Y. Pada Gambar 4.23 terlihat bahwa titik-titik data menyebar secara acak tanpa membentuk pola tertentu, seperti pola bergelombang, pola melebar lalu menyempit (*funnel shape*), atau pola geometris lainnya. Selain itu, persebaran titik tampak merata di area positif maupun negatif pada sumbu Y. Pola sebaran yang acak dan tidak teratur tersebut menunjukkan bahwa varians residual antar pengamatan bersifat konstan (homoskedastisitas).

b. Hasil Uji menggunakan RStudio

```
[1] ">>> Hasil Uji Heteroskedastisitas (Breusch-Pagan):"
> print(bptest(model_revised))

        studentized Breusch-Pagan test

data:  model_revised
BP = 7.2098, df = 4, p-value = 0.1252
```

Gambar 4. 24 Hasil Uji Heteroskedastisitas dengan RStudio

Berdasarkan hasil uji heteroskedastisitas pada Gambar 4.24, diperoleh nilai *p-value* sebesar 0,1252. Karena nilai tersebut lebih besar dari 0,05 (0,1252 > 0,05), maka dapat disimpulkan bahwa model regresi tidak mengalami masalah heteroskedastisitas. Dengan demikian, varians residual pada setiap tingkat variabel independen bersifat homogen atau memenuhi asumsi homoskedastisitas.

Berdasarkan hasil pengujian heteroskedastisitas yang dilakukan menggunakan dua alat analisis, terlihat kesamaan hasil antara SPSS dan RStudio. Berdasarkan hasil pengujian heteroskedastisitas yang dilakukan menggunakan SPSS melalui analisis *scatterplot* pada Gambar 4.23, dapat dilihat bahwa titik-titik residual menyebar secara acak di sekitar garis horizontal tanpa membentuk pola tertentu. Pola penyebaran yang acak ini menunjukkan bahwa varian residual bersifat konstan (homoskedastisitas) dan tidak terdapat indikasi gejala heteroskedastisitas pada model regresi. Sementara itu Gambar 4.24 menunjukkan hasil uji Breusch-Pagan *Test* pada RStudio menunjukkan nilai *p-value* sebesar 0,1252 (> 0,05), sehingga dapat disimpulkan bahwa model regresi secara keseluruhan tidak mengalami masalah heteroskedastisitas. Dengan demikian, dapat disimpulkan bahwa model regresi memenuhi asumsi klasik heteroskedastisitas, sehingga hasil estimasi regresi dapat dianggap valid.

4.4 Analisis Regresi Linier Berganda

Analisis regresi linier berganda digunakan untuk mengetahui pengaruh variabel independen (Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko) terhadap variabel dependen (Perilaku Keamanan Kata Sandi).

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	816.260	4	204.065	5.608	<,001[b]
	Residual	3456.650	95	36.386		
	Total	4272.910	99			

a. Dependent Variable: Y1

b. Predictors: (Constant), X4, X1, X2, X3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-61.740	18.774		-3.289	.001
	X1	.597	.298	.187	2.002	.048
	X2	1.269	.530	.223	2.394	.019
	X3	1.329	.405	.312	3.284	.001
	X4	.555	.269	.196	2.061	.042

a. Dependent Variable: Y1

Gambar 4. 25 Hasil Analisis Regresi Linier Berganda menggunakan SPSS

```
Call:
lm(formula = Perilaku_Keamanan_Kata_Sandi ~ Kecemasan_Ingatan +
    Pengaruh_Teman_Sebaya + Pengalaman_Keamanan_Siber_Pribadi +
    Persepsi_Risiko, data = data)

Residuals:
    Min      1Q  Median      3Q     Max
-1.2591 -0.4257 -0.1040  0.1883  6.7600

Coefficients:
                                Estimate Std. Error t value Pr(>|t|)
(Intercept)                     -10.2900     3.1290  -3.289  0.00141 **
Kecemasan_Ingatan                 0.4973     0.2484   2.002  0.04813 *
Pengaruh_Teman_Sebaya             1.2691     0.5302   2.394  0.01864 *
Pengalaman_Keamanan_Siber_Pribadi 1.3289     0.4047   3.284  0.00144 **
Persepsi_Risiko                   0.4627     0.2244   2.061  0.04200 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.005 on 95 degrees of freedom
Multiple R-squared:  0.191,     Adjusted R-squared:  0.157
F-statistic: 5.608 on 4 and 95 DF,  p-value: 0.0004265
```

Gambar 4. 26 Hasil Analisis Regresi Linier Berganda menggunakan RStudio

Berdasarkan hasil analisis pada Gambar 4.25 dan Gambar 4.26, baik menggunakan RStudio maupun SPSS, diperoleh hasil yang konsisten, di mana nilai F-statistic sebesar 5,608 dengan *p-value* < 0,001 menunjukkan bahwa model regresi signifikan secara simultan. Selain itu, hasil uji parsial juga menunjukkan bahwa seluruh variabel independen (X1, X2, X3, X4) memiliki nilai Sig. < 0,05 dan nilai t hitung lebih besar dari t tabel (1,660), yang berarti masing-

masing variabel berpengaruh signifikan terhadap variabel dependen. Dengan demikian, kedua alat analisis menghasilkan interpretasi yang sejalan, yaitu seluruh variabel independen secara parsial maupun simultan berpengaruh signifikan terhadap perilaku keamanan kata sandi.

Tabel 4. 5 Hasil Kesimpulan Analisis Regresi Linier Berganda

Variabel	Estimate	Std. Error	t-value	p-value (Sig.)
(Intercept)	-10.290	3.129	-3.289	0.00141
Kecemasan Memori (X1)	0.497	0.248	2.002	0.04813
Pengaruh Teman Sebaya (X2)	1.269	0.530	2.394	0.01864
Pengalaman Keamanan Siber Pribadi (X3)	1.328	0.404	3.284	0.00144
Persepsi Risiko (X4)	0.462	0.224	2.061	0.04200

Dalam analisis regresi, (*Intercept*) menunjukkan nilai dasar variabel dependen ketika seluruh variabel independen bernilai nol. Estimate menggambarkan besarnya dan arah pengaruh tiap variabel independen, sementara *Std. Error* menunjukkan seberapa jauh nilai estimasi dapat menyimpang dari nilai sebenarnya. Signifikansi pengaruh diuji melalui t-value dan p-value, di mana variabel dinyatakan berpengaruh signifikan apabila p-value < 0,10.

a. Tabel 4.5 menunjukan nilai konstanta sebesar -10,290 menunjukkan bahwa apabila seluruh variabel independen, yaitu Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko berada pada nilai nol, maka Perilaku Keamanan Kata Sandi diperkirakan sebesar -10,290. Secara praktis, konstanta yang bernilai negatif ini menandakan bahwa tanpa adanya pengaruh dari keempat variabel tersebut, tingkat perilaku keamanan kata sandi cenderung sangat rendah atau bahkan tidak muncul.
b. Berdasarkan hasil analisis regresi linier berganda pada Tabel 4.5 bahwa variabel Kecemasan Ingatan (X1) memiliki nilai koefisien sebesar 0,497, nilai t-hitung 2,002, dan nilai signifikansi (*p-value*) 0,04813. Karena nilai signifikansi (0,04813 < 0,10) dan t-hitung (2,002) > t-tabel (1,660), yang berarti variabel Kecemasan Ingatan berpengaruh

signifikan terhadap Perilaku Keamanan Kata Sandi. Namun demikian, arah pengaruh yang dihasilkan positif (0,497), berbeda dengan dugaan awal yang memperkirakan pengaruh negatif. Hal ini menunjukkan bahwa semakin tinggi tingkat kecemasan terhadap ingatan kata sandi, semakin baik perilaku keamanan kata sandi yang diterapkan siswa.

c. Hasil regresi linier berganda pada Tabel 4.5 menunjukkan bahwa variabel Pengaruh Teman Sebaya (X2) memiliki nilai koefisien sebesar 1,269, nilai t-hitung 2,394, dan nilai signifikansi (*p-value*) 0,01864. Karena nilai signifikansi (0,01864 < 0,10), t-hitung (2,394) > t-tabel (1,660), dan arah koefisien positif (1,269), dapat disimpulkan bahwa pengaruh teman sebaya berkontribusi positif dan signifikan terhadap perilaku keamanan kata sandi. Artinya, semakin kuat pengaruh positif dari lingkungan pertemanan, semakin baik pula praktik keamanan kata sandi yang diterapkan oleh siswa.

d. Berdasarkan hasil analisis regresi linier berganda pada Tabel 4.5 bahwa variabel Pengalaman Keamanan Siber Pribadi (X3) memiliki nilai koefisien sebesar 1,328, nilai t-hitung 3,284, dan nilai signifikansi (*p-value*) 0,00144. Karena nilai signifikansi (0,00144 < 0,05), t-hitung (3,284) > t-tabel (1,660) dan arah koefisien positif (1,328) menunjukkan bahwa pengalaman pribadi dalam menghadapi insiden keamanan siber berpengaruh positif dan signifikan terhadap perilaku keamanan kata sandi. Dengan kata lain, siswa yang memiliki pengalaman langsung terkait pelanggaran keamanan digital cenderung lebih berhati-hati dalam mengelola kata sandinya.

e. Hasil regresi linier berganda pada Tabel 4.5 menunjukkan bahwa variabel Persepsi Risiko (X4) memiliki nilai koefisien sebesar 0,462, nilai t-hitung 2,061, dan nilai signifikansi (*p-value)* 0,04200. Karena nilai signifikansi (0,04200 < 0,10), t-hitung (2,061) > t-tabel (1,660) dengan koefisien positif (0,462) menunjukkan bahwa semakin tinggi persepsi risiko terhadap ancaman keamanan digital, semakin baik perilaku keamanan kata sandi yang diterapkan siswa. Hal ini mengindikasikan bahwa kesadaran terhadap potensi risiko berperan penting dalam mendorong tindakan pencegahan yang lebih kuat.

4.4.1 Uji Simultan (Uji-f)

Tabel 4. 6 Hasil Koefisien Determinasi dan Uji F dengan Regresi Linier Berganda

Statistik Model	Nilai
Multiple R-squared	0.191
Adjusted R-squared	0.157
F-statistic	5.608

Berdasarkan hasil analisis pada Tabel 4.6, diperoleh nilai F-statistic sebesar 5,608 dengan derajat kebebasan (df) 4 dan 90 serta *p-value* sebesar 0,0004265. Dengan tingkat signifikansi α = 0,10, karena *p-value* (0,0004265) lebih kecil dari α (0,10), maka dapat disimpulkan bahwa model regresi linier berganda yang digunakan dalam penelitian ini layak dan dapat dimanfaatkan untuk memprediksi Perilaku Keamanan Kata Sandi. Artinya, secara simultan variabel Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko memiliki pengaruh yang signifikan terhadap Perilaku Keamanan Kata Sandi pada siswa SMA/SMK sederajat di Provinsi DIY.

4.4.2 Uji Parsial (Uji-t)

Uji t dilakukan untuk mengetahui pengaruh masing-masing variabel independen secara parsial terhadap variabel dependen. Pengujian dilakukan dengan membandingkan nilai t-hitung dengan t-tabel (1,660) atau dengan melihat nilai signifikansi (*p-value*) dengan tingkat kepercayaan 90% (α = 0,10). Kriteria pengujian yang digunakan yaitu:

a. Jika t-hitung > t-tabel (1,660) atau *p-value* < 0,10, maka H_0 ditolak dan H_a diterima (variabel independen berpengaruh signifikan)
b. Jika t-hitung < t-tabel (1,660) atau *p-value* > 0,10, maka H_0 diterima dan H_a ditolak (variabel independen tidak berpengaruh signifikan)

Dapat disimpulkan bahwa hipotesis, sebagai berikut:

a. Hipotesis 1: Pengaruh Kecemasan Ingatan terhadap Perilaku Keamanan Kata Sandi
    1. H_0: Kecemasan Ingatan tidak berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi
    2. H_a: Kecemasan Ingatan berpengaruh positif signifikan terhadap Perilaku Keamanan Kata Sandi

Berdasarkan hasil uji t diperoleh nilai t-hitung sebesar 2,002 yang lebih besar dari t-tabel 1,660 serta *p-value* sebesar 0,04813 yang lebih kecil dari tingkat signifikansi α = 0,10. Dengan demikian, H_0 ditolak dan H_a diterima , yang berarti bahwa variabel Kecemasan Ingatan berpengaruh positif dan signifikan terhadap Perilaku Keamanan Kata Sandi pada siswa SMA/SMK sederajat di Provinsi Daerah Istimewa Yogyakarta.

Hasil ini menunjukkan bahwa semakin tinggi tingkat kecemasan siswa terhadap kemampuan mereka dalam mengingat kata sandi, semakin baik pula perilaku keamanan kata sandi yang mereka terapkan. Meskipun hipotesis awal menduga adanya pengaruh negatif bahwa kecemasan terhadap ingatan akan menurunkan perilaku keamanan karena siswa mungkin memilih kata sandi yang sederhana agar mudah diingat. Hal ini dapat dijelaskan oleh

meningkatnya literasi digital dan kesadaran keamanan di kalangan siswa, di mana mereka tidak hanya cemas akan lupa, tetapi juga memahami pentingnya menjaga keamanan akun digital. Akibatnya, kecemasan tersebut menjadi stimulus positif yang mendorong kehati-hatian dan perilaku keamanan yang lebih baik.

b. Hipotesis 2: Pengaruh Teman Sebaya terhadap Perilaku Keamanan Kata Sandi
    1. H_0: Pengaruh Teman Sebaya tidak berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi
    2. H_a: Pengaruh Teman Sebaya berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi

Berdasarkan hasil uji t diperoleh nilai t-hitung sebesar 2,394 yang lebih besar dari t-tabel 1,660 serta *p-value* sebesar 0,01864 yang lebih kecil dari tingkat signifikansi $\alpha = 0{,}10$. Dengan demikian, H_0 ditolak dan H_a diterima. Hasil ini menunjukkan bahwa variabel Pengaruh Teman Sebaya berpengaruh positif dan signifikan terhadap Perilaku Keamanan Kata Sandi pada siswa SMA/SMK sederajat di Provinsi Daerah Istimewa Yogyakarta. Artinya, semakin besar pengaruh positif dari teman sebaya dalam hal keamanan kata sandi, semakin baik pula perilaku keamanan kata sandi yang diterapkan oleh siswa. Temuan ini menegaskan bahwa faktor lingkungan sosial, khususnya kelompok pertemanan, berperan penting dalam membentuk perilaku keamanan digital siswa, di mana mereka cenderung meniru atau menyesuaikan praktik keamanan yang dilakukan oleh teman-teman di sekitar mereka.

c. Hipotesis 3: Pengaruh Pengalaman Keamanan Siber Pribadi terhadap Perilaku Keamanan Kata Sandi
    1. H_0: Pengalaman Keamanan Siber Pribadi tidak berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi
    2. H_a: Pengalaman Keamanan Siber Pribadi berpengaruh positif signifikan terhadap Perilaku Keamanan Kata Sandi

Berdasarkan hasil uji t diperoleh nilai t-hitung sebesar 3,284 yang lebih besar dari t-tabel 1,660 serta *p-value* sebesar 0,00144 yang lebih kecil dari tingkat signifikansi $\alpha = 0{,}10$. Dengan demikian, H_0 ditolak dan H_a diterima. Hasil ini menunjukkan bahwa variabel Pengalaman Keamanan Siber Pribadi berpengaruh positif dan signifikan terhadap Perilaku Keamanan Kata Sandi pada siswa SMA/SMK sederajat di Provinsi Daerah Istimewa Yogyakarta. Dengan nilai t-hitung tertinggi (3,284) dan *p-value* terendah (0,00144), variabel ini menjadi prediktor paling kuat dalam penelitian ini. Temuan tersebut mengindikasikan bahwa siswa yang memiliki pengalaman langsung terkait insiden keamanan siber, seperti peretasan akun, phishing, atau

kehilangan data, cenderung lebih sadar dan menerapkan perilaku keamanan kata sandi yang lebih baik. Pengalaman pribadi semacam ini berperan sebagai pembelajaran nyata yang efektif dalam membentuk kesadaran dan kebiasaan keamanan digital siswa.

d. Hipotesis 4: Pengaruh Persepsi Risiko terhadap Perilaku Keamanan Kata Sandi
    1. H_0: Persepsi Risiko tidak berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi
    2. H_a: Persepsi Risiko berpengaruh positif signifikan terhadap Perilaku Keamanan Kata Sandi

Berdasarkan hasil uji t diperoleh nilai t-hitung sebesar 2,061 yang lebih besar dari t-tabel 1,660 serta *p-value* sebesar 0,04200 yang lebih kecil dari tingkat signifikansi $\alpha = 0{,}10$. Dengan demikian, H_0 ditolak dan H_a diterima. Hasil ini menunjukkan bahwa variabel Persepsi Risiko berpengaruh positif dan signifikan terhadap Perilaku Keamanan Kata Sandi pada siswa SMA/SMK sederajat di Provinsi DIY. Artinya, semakin tinggi persepsi siswa terhadap risiko yang terkait dengan keamanan siber, semakin baik pula perilaku keamanan kata sandi yang mereka terapkan. Siswa yang memiliki kesadaran akan potensi ancaman digital cenderung lebih berhati-hati dan proaktif dalam melindungi akun serta data pribadi mereka, misalnya dengan menggunakan kata sandi yang kuat dan menerapkan langkah-langkah keamanan yang lebih baik.

Hasil penelitian menunjukkan bahwa seluruh variabel independen berpengaruh positif dan signifikan terhadap Perilaku Keamanan Kata Sandi siswa SMA/SMK sederajat di Provinsi DIY. Menariknya, variabel Kecemasan Ingatan menunjukkan arah pengaruh yang berbeda dari hipotesis awal yang memprediksi hubungan negatif. Temuan ini mengindikasikan bahwa siswa yang merasa cemas akan lupa kata sandi justru lebih berhati-hati dan cenderung menerapkan praktik keamanan yang lebih baik. Secara keseluruhan, hasil penelitian ini konsisten dengan temuan terdahulu yang menegaskan bahwa faktor psikologis, sosial, dan pengalaman digital berperan penting dalam membentuk perilaku keamanan. Hal ini menunjukkan bahwa generasi muda di Provinsi DIY telah memiliki kesadaran dan sikap yang adaptif terhadap keamanan digital di era teknologi yang semakin berkembang.

4.4.3 Koefisien Determinasi (R^2)

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.437[a]	.191	.157	6.03206

a. Predictors: (Constant), X4, X1, X2, X3

b. Dependent Variable: Y1

Gambar 4. 27 Hasil Uji Koefisien Determinasi menggunakan SPSS

Hasil analisis regresi yang ditampilkan pada Tabel 4.6 (menggunakan RStudio) dan Gambar 4.27 (menggunakan SPSS) menunjukkan bahwa nilai *Multiple R-squared* sebesar 0,191 dan *Adjusted R-squared* sebesar 0,157. Nilai *Adjusted R-squared* sebesar 0,157 atau 15,7% mengindikasikan bahwa variabel independen, yaitu Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko, secara bersama-sama mampu menjelaskan 15,7% variasi dari variabel dependen, yaitu Perilaku Keamanan Kata Sandi. Sementara itu, sebesar 84,3% variasi lainnya dijelaskan oleh faktor-faktor di luar model penelitian, seperti tingkat literasi digital, pelatihan keamanan siber, kebijakan sekolah, maupun karakteristik demografis lainnya. Nilai koefisien determinasi yang relatif rendah ini menunjukkan bahwa masih terdapat banyak faktor eksternal yang berpotensi memengaruhi perilaku keamanan kata sandi pada siswa SMA/SMK di Provinsi DIY.

4.5 Interpretasi Hasil Penelitian

Analisis deskriptif menunjukkan bahwa tingkat kesadaran siswa terhadap pentingnya keamanan kata sandi tergolong baik, dengan rata-rata keseluruhan 4,12 dari skala 5. Kesadaran tertinggi terlihat pada aspek perilaku dasar keamanan, seperti tidak membagikan kata sandi akun sekolah kepada teman (rata-rata 4,38) dan menggunakan kombinasi huruf, angka, serta simbol dalam pembuatan kata sandi (rata-rata 4,29). Keduanya termasuk kategori sangat baik.

Namun, masih terdapat aspek yang perlu ditingkatkan, khususnya dalam hal kewaspadaan terhadap ancaman rekayasa sosial seperti *phishing* melalui tautan email mencurigakan, yang memiliki nilai terendah 3,86. Hal ini menunjukkan bahwa meskipun siswa sudah memiliki dasar kesadaran keamanan yang cukup baik, masih dibutuhkan peningkatan pemahaman dalam mengenali dan merespons ancaman siber yang lebih kompleks, serta pentingnya menggunakan kata sandi unik untuk setiap akun agar risiko kebocoran data dapat diminimalkan.

Hasil validasi instrumen penelitian menunjukkan bahwa seluruh butir kuesioner dinyatakan valid dan reliabel, dengan nilai signifikansi di bawah 0,05 pada uji validitas dan nilai Cronbach's Alpha di atas 0,70 untuk semua variabel. Konsistensi hasil antara SPSS dan RStudio memperkuat keandalan data yang digunakan. Selain itu, hasil uji asumsi klasik menunjukkan bahwa model regresi memenuhi seluruh kriteria statistik yang diperlukan untuk menghasilkan estimasi yang akurat (*Best Linear Unbiased Estimator*). Uji normalitas residual menggunakan Kolmogorov-Smirnov menunjukkan nilai *p-value* di atas 0,05, hubungan antarvariabel terbukti linear dengan Deviation from Linearity di atas 0,05, tidak ditemukan gejala multikolinearitas karena seluruh nilai VIF < 10, dan model bebas dari heteroskedastisitas berdasarkan Breusch-Pagan *Test* dengan *p-value* sebesar 0,1252. Dengan demikian, model yang digunakan dapat dipercaya dan hasil estimasinya tidak bias.

Hasil analisis regresi linier berganda menunjukkan bahwa keempat variabel independen (Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko) secara simultan berpengaruh signifikan terhadap Perilaku Keamanan Kata Sandi, dengan nilai F-statistic sebesar 5,608 dan *p-value* < 0,001. Secara parsial, seluruh variabel berpengaruh positif dan signifikan terhadap perilaku keamanan kata sandi. Menariknya, variabel Kecemasan Ingatan menunjukkan arah pengaruh yang berbeda dari hipotesis awal. Awalnya diasumsikan bahwa kecemasan terhadap kemampuan mengingat kata sandi akan berdampak negatif karena siswa mungkin memilih kata sandi sederhana agar mudah diingat. Namun, hasil penelitian justru menunjukkan pengaruh positif. Hal ini mengindikasikan bahwa rasa cemas terhadap kemungkinan lupa mendorong siswa untuk lebih berhati-hati dan proaktif dalam mengelola kata sandi. Di sisi lain, Pengalaman Keamanan Siber Pribadi merupakan faktor paling kuat, menegaskan bahwa pengalaman langsung menghadapi insiden siber menjadi pembelajaran paling efektif dalam membentuk perilaku keamanan siswa. Selain itu, Pengaruh Teman Sebaya juga memiliki pengaruh besar, menandakan bahwa dukungan sosial dan norma kelompok sangat berperan dalam membentuk kebiasaan keamanan digital di kalangan remaja. Sementara itu, Persepsi Risiko berkontribusi positif dengan menunjukkan bahwa semakin tinggi kesadaran siswa terhadap potensi ancaman digital, semakin baik pula perilaku keamanan yang mereka terapkan.

Meskipun model penelitian ini signifikan, nilai *Adjusted R-squared* sebesar 0,157 (15,7%) menunjukkan bahwa masih terdapat 84,3% faktor lain di luar model yang memengaruhi perilaku keamanan kata sandi, seperti tingkat literasi digital, kebijakan sekolah, paparan terhadap edukasi keamanan siber, maupun faktor demografis.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, tingkat kesadaran siswa SMA/SMK sederajat di Provinsi DIY terhadap pentingnya keamanan kata sandi dalam kehidupan digital berada pada kategori baik, dengan nilai rata-rata keseluruhan sebesar 4,12 dari skala 5. Siswa telah menunjukkan penerapan praktik keamanan dasar yang cukup kuat, terutama dalam menjaga kerahasiaan kata sandi (nilai 4,38) dan menggunakan kombinasi huruf, angka, serta simbol dalam pembuatan kata sandi (nilai 4,29). Namun, masih ditemukan kelemahan pada aspek keamanan yang lebih kompleks, seperti kewaspadaan terhadap ancaman eksternal. Hal ini terlihat dari nilai terendah sebesar 3,86, yang menunjukkan bahwa sebagian siswa masih kurang berhati-hati terhadap tautan mencurigakan dalam email atau bentuk serangan rekayasa sosial lainnya.

Selanjutnya, hasil analisis terhadap faktor-faktor yang memengaruhi perilaku keamanan kata sandi menunjukkan bahwa keempat variabel independen (Kecemasan Ingatan, Pengaruh Teman Sebaya, Pengalaman Keamanan Siber Pribadi, dan Persepsi Risiko) secara simultan maupun parsial berpengaruh positif dan signifikan terhadap perilaku keamanan kata sandi siswa. Menariknya, Kecemasan Ingatan menunjukkan arah pengaruh yang berbeda dari hipotesis awal yang memperkirakan hubungan negatif. Hasil penelitian justru mengungkap bahwa semakin tinggi tingkat kecemasan siswa terhadap kemampuan mengingat kata sandi, semakin baik pula perilaku keamanan yang diterapkan. Hal ini mengindikasikan bahwa kekhawatiran akan lupa kata sandi dapat mendorong siswa untuk lebih berhati-hati dan menerapkan strategi keamanan yang lebih efektif. Di antara keempat variabel tersebut, Pengalaman Keamanan Siber Pribadi menjadi faktor paling dominan (nilai t = 3,284), yang menegaskan bahwa pengalaman langsung menghadapi insiden keamanan siber berperan penting dalam membentuk perilaku yang lebih waspada dan sadar risiko. Dengan demikian, hasil ini memperlihatkan bahwa siswa di Provinsi DIY cenderung belajar dari pengalaman nyata dan lingkungan sosialnya, sehingga mampu merespons tantangan keamanan digital dengan cara yang lebih adaptif dan bertanggung jawab.

5.2 Saran

Berdasarkan temuan empiris yang diperoleh, beberapa rekomendasi dapat diajukan bagi pihak sekolah dan peneliti berikutnya. Pertama, karena skor terendah terdapat pada aspek kewaspadaan terhadap tautan mencurigakan (rata-rata 3,86), sekolah perlu memperkuat edukasi melalui simulasi visual atau latihan identifikasi tautan mecurigakan agar siswa lebih terampil mengenali upaya rekayasa sosial. Kedua, mengingat variabel Pengalaman Keamanan Siber Pribadi merupakan faktor paling dominan yang memengaruhi perilaku keamanan kata sandi, pendekatan pembelajaran dianjurkan beralih dari metode ceramah menjadi penyajian studi kasus atau demonstrasi kejadian nyata untuk menumbuhkan pengalaman konseptual yang lebih bermakna. Ketiga, hasil bahwa Kecemasan Ingatan berpengaruh positif menunjukkan bahwa tingkat kekhawatiran yang terkelola dapat mendorong praktik keamanan yang lebih baik. Oleh karena itu, pendidik disarankan menumbuhkan kewaspadaan yang sehat melalui penekanan pada pentingnya kehati-hatian dan konsistensi dalam menjaga keamanan akun.

DAFTAR PUSTAKA

Adewusi, M. A., Odekeye, O. T., & Wasiu, A. A. (2024). *Understanding Online Security Perceptions and Practices: A Qualitative Study*. *13*. https://www.researchgate.net/publication/384830311

Aini, A. N., Wahyudi, E., & Abdillah, I. (2022). Model Perilaku Keamanan Siber Pada Pengguna Sosial Media Pada Masa Pandemi Covid-19. *Jurnal Teknologi Informasi Dan Terapan*, *9*(1), 37–40. https://doi.org/10.25047/jtit.v9i1.272

Albone, A. (2009). *PEMBUATAN RENCANA KEAMANAN INFORMASI BERDASARKAN ANALISIS DAN MITIGASI RISIKO TEKNOLOGI INFORMASI*.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052589

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing*. https://doi.org/10.3390/bdcc7020073

Antoro, B. (2024). ANALISIS PENERAPAN FORMULA SLOVIN DALAM PENELITIAN ILMIAH: KELEBIHAN, KELEMAHAN, DAN KESALAHAN DALAM PERSPEKTIF STATISTIK. *JURNAL Multidisiplin Sosial Dan Humaniora*, *1*(2). https://doi.org/https://doi.org/10.70585/jmsh.v1i2.38

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Ariyanto, D., & Rachmadiarti, F. (2022). PENINGKATAN KEMAMPUAN ANALISIS STATISTIK MENGGUNAKAN APLIKASI R STUDIO BERBASIS OPEN SOURCE UNTUK KEBUTUHAN PENELITIAN DOSEN DI FAKULTAS MIPA UNIVERSITAS NEGERI SURABAYA. *Jurnal Umum Pengabdian Masyarakat*.

Aulia, R. E., Sumiharsono, R., & Triwahyuni, E. (2023). *Pengaruh Penggunaan Modul IPA Berbasis Problem Based Learning (PBL) Terhadap Keterampilan Proses Sains Dan Keterampilan Berpikir Kritis Siswa (The Effect of Using Problem Based Learning (PBL) Natural Sciences Modules on Students' Science Process Skills a*. *4*, 1445–1454. https://doi.org/https://doi.org/10.62775/edukasia.v4i2.459

Ayyagari, R., Lim, J., & Hoxha, O. (2020). Why do not we use password managers? A study on the intention to use password managers. *Contemporary Management Research*, *15*(4), 227–245. https://doi.org/10.7903/cmr.19394

Bhana, B., & Flowerday, S. V. (2021). Usability of the login authentication process: passphrases and passwords. *Information and Computer Security*, *30*(2), 280–305. https://doi.org/10.1108/ICS-07-2021-0093

Blažič, B. J., & Blažič, A. J. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability*. https://doi.org/10.3390/su14084763

Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity Awareness, and Cybersecurity Behavior of High School Students in Davao City: A Mediation Role of Perceived Behavioral Control. *European Journal of Applied Science, Engineering and Technology*, *2*(3), 4–9. https://doi.org/10.59324/ejaset.2024.2(3).01

Bujang, M. A., Omar, E. D., Foo, D. H. P., & Hon, Y. K. (2024). Sample size determination for conducting a pilot study to assess reliability of a questionnaire. In *Restorative Dentistry and Endodontics* (Vol. 49, Issue 1). Korean Academy of Conservative Dentistry. https://doi.org/10.5395/rde.2024.49.e3

Cicilia Warayaan, B. (2025). PENGARUH E-FILING, PRIVASI DAN KEAMANAN, KESADARAN WAJIB PAJAK TERHADAP KEPATUHAN WAJIB PAJAK ORANG PRIBADI. *Oktober*, *5*(2), 1161–1172. https://doi.org/10.25105/jet.v5i2.23088

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi Dan Informasi (JATI)*, *12*(27), 12. https://doi.org/10.34010/jati.v12i2

Dinas Komunikasi dan Informatika Kabupaten Ngawi. (2023, October). *Sosialisasi keamanan informasi bagi pelajar SMAN 1 Ngawi*. https://kominfo.ngawikab.go.id/sosialisasi-keamanan-informasi-bagi-pelajar-sman-1-ngawi/

Doria, J. D. (2024). Factors Influencing Employees' Information Security Behavior in the Telework Environment: An Empirical Study of the Philippines. *International Journal of Research Publications*, *156*, 37–55. https://doi.org/10.47119/IJRP1001561920247139

Dupuis, M., & Khan, F. (2018). Effects of peer feedback on password strength. *2018 APWG Symposium on Electronic Crime Research (ECrime)*, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

Dwi Madya, A., Djoko Haryanto, B., Ningsih, D. P., & Sinlae, F. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *INDOTECH Indonesian Journal of Education And Computer Science*, *1*(3), 2023.

Fauzi, M. R. (2024). Analisis Tingkat Security Awareness Dalam Password Behavior Mahasiswa (Studi Kasus Mahasiswa FEBI UINSU Medan). *JPEK (Jurnal Pendidikan Ekonomi Dan Kewirausahaan)*, *8*(3). https://doi.org/10.29408/jpek.v8i3.29304

Fermayani, R., Harahap, R. R., & Rahmat, R. (2022). *ANALISIS PENGARUH PRIVASI, KEAMANAN, DAN KEPERCAYAAN TERHADAP NIAT UNTUK BERTRANSAKSI SECARA ONLINE DI LAZADA*. *8*(1).

Fitria, K. M. (2023). ANALISIS SERANGAN MALWARE DALAM PERBANKAN DAN PERENCANAAN SOLUSI KEAMANAN. *Jurnal Informatika Dan Teknik Elektro Terapan*, *11*(3). https://doi.org/10.23960/jitet.v11i3.3312

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism*, *10*(2), 486–489. https://doi.org/10.5812/ijem.3505

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Habagat, J. B. A., & Hermosa, J. P. (2024). *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY : APPLIED Authentic Assessment in Flexible Learning Modality and the Learning Outcomes in Readings in the Philippine History Among First-Year College Students*. *5*(10), 3968–3989. https://doi.org/10.11594/ijmaber.05.10.15

Hadzidedic, S., Fajardo-Flores, S., & Ramic-Brkic, B. (2022). User perceptions and use of authentication methods: insights from youth in Mexico and Bosnia and Herzegovina. *Information and Computer Security*, *30*(4), 615–632. https://doi.org/10.1108/ICS-07-2021-0105

Handayani, M., Jayadilaga, Y., Fitri, A. U., Rachman, D. A., Istiqamah, N. F., T.A, T. D., Pratiwi, A. P., & Kas, S. R. (2023). Sosialisasi dan Pengenalan Aplikasi Pengolahan Data SPSS pada Mahasiswa Administrasi Kesehatan Fakultas Ilmu Keolahragaan dan Kesehatan. *JIPM : Jurnal Informasi Pengabdian Masyarakat*, *1*(2). https://e-journal.nalanda.ac.id/index.php/jipm

Herlambang, P. M., Anjani, S., Wijayanto, H., & Murni, M. (2020). Cyber Security Behavior Model on Health Information System Users During Covid-19 Pandemic. *Cyber Security Dan Forensik Digital*, *3*(2), 27–33. https://doi.org/10.14421/csecurity.2020.3.2.2152

Iba, Z., & Wardhana, A. (2024). *Analisis Regresi dan Analisis Jalur Untuk Riset Bisnis Menggunakan SPSS 29.0 & SMART-PLS 4.0* (M. Pradana, Ed.; 1st ed.). EUREKA MEDIA AKSARA, JUNI 2024 ANGGOTA IKAPI JAWA TENGAH NO. 225/JTE/2021.

Indrayani, R. (2020). Pelatihan Pengamanan Data Cyberspace untuk Siswa Sekolah Lanjutan Tingkat Atas. *Muria Jurnal Layanan Masyarakat*.

Iqbal, F., Nawaz, S. A., Aslam, T., Ahmad, R. N., & Ijaz, H. M. (2024). *Impact of Cyber Security Measures in The Digital Banking Sec- tor of Pakistan*. *XX*(Xx).

Kementerian Pendidikan Dasar dan Menengah. (2025). *Data Pokok Pendidikan Nasional*. Https://Dapo.Kemendikdasmen.Go.Id/Pd/1/040000.

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, *11*(November). https://doi.org/10.3389/fpsyg.2020.546546

Kim, J., & Kang, D. (2008). *A Study on the Factors Affecting the Information Systems Security Effectiveness of Password*.

Kwak, S. G., & Kim, J. H. (2017). Central limit theorem: The cornerstone of modern statistics. *Korean Journal of Anesthesiology*, *70*(2), 144–156. https://doi.org/10.4097/kjae.2017.70.2.144

Luna, K. (2019). If it is easy to remember, then it is not secure: Metacognitive beliefs affect password selection. *Applied Cognitive Psychology*, *33*(5), 744–758. https://doi.org/https://doi.org/10.1002/acp.3516

Mahendra, A. F., Hatta, P., & Aristyagama, Y. H. (2024). Analisis Tingkat Kesadaran Keamanan Cyber di Media Sosial Instagram: Studi Kasus pada Siswa SMK Negeri 1 Banyudono. *Bina Insani Ict Journal*, *11*(1), 86. https://doi.org/10.51211/biict.v11i1.2963

Mamduh Mohamad. (2024, December 19). *Kebutuhan Mendesak untuk Tingkatkan Keamanan Siber di Sekolah*. Https://Www.Medcom.Id/Teknologi/News-Teknologi/ANrjvAEN-Kebutuhan-Mendesak-Untuk-Tingkatkan-Keamanan-Siber-Di-Sekolah.

Mariani. (2018). *PENGARUH PENGGUNAAN MEDIA VISUAL TERHADAP MINAT BELAJAR SISWA PADA MATA PELAJARAN PRAKARYA DAN KEWIRAUSAHAAN JURUSAN AKUNTANSI DI SEKOLAH MENENGAH KEJURUAN MUHAMMADIYAH 2 PEKANBARU* [Skripsi thesis]. Universitas Islam Negeri Sultan Syarif Kasim Riau.

Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty*.

Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X). *JURNAL SISTEM INFORMASI BISNIS*, *6*(2), 97. https://doi.org/10.21456/vol6iss2pp97-104

Muhazzab, A. F., Zelyn, F., Binti Nur, A., & Rokhmat, S. (2023). *ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI*. *5*(2), 2023. https://doi.org/https://doi.org/10.47435/asy-syarikah.v5i2.2022

Mwagwabi, F., & Hee Jiow, J. (2021). Compliance with security guidelines in teenagers: the conflicting role of peer influence and personal norms. In *Australasian Journal of Information Systems Mwagwabi & Hee Jiow* (Vol. 25).

Novianto, E., Heri Ujianto, E. I., & Rianto, R. (2023). KEAMANAN INFORMASI (INFORMATION SECURITY) PADA APLIKASI SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN DEFENSE IN DEPTH. *Jurnal Komputer Dan Informatika*, *11*(1), 1–6. https://doi.org/10.35508/jicon.v11i1.9139

Nursiah, N., Ferils, M., & Kamarudin, J. (2022). Analisis minat menggunakan mobile banking. *AKUNTABEL*, *19*, 91–100. https://doi.org/10.30872/jakt.v19i1.10711

Pakpahan, A. P., Heing, B. D. W., Pane, C. G. G., Purba, A. R., Pujabramantya, A., & Nastiti, P. (2021). *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi Edukasi Pada Siswa SMA Negeri 1 Mimika untuk Mengatasi Ancaman Media Online pada Data Pribadi*.

Peker, Y. K., Ray, L., & Da Silva, S. (2018). Online cybersecurity awareness modules for college and high school students. *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, 24–33. https://doi.org/10.1109/NCS.2018.00009

Pickering, B., & Taylor, S. (2025). *Individual Perceptions of Cybersecurity and Risk Management*. https://doi.org/10.12688/openreseurope.17332.1

Poornachandran, P., Nithun, M., Pal, S., Ashok, A., & Ajayan, A. (2016). Password Reuse Behavior: How Massive Online Data Breaches Impacts Personal Data in Web. In H. S. Saini, R. Sayal, & S. S. Rawat (Eds.), *Innovations in Computer Science and Engineering* (pp. 199–210). Springer Singapore.

Putri, I., Agita, A., & Soim, S. (2023). Implementasi Port Knocking, Port Blocking Pada Keamanan Jaringan Komputer Berbasis Mikrotik. *Journal |*, *125*. https://s.id/jurnalresistor

Raharjo, B. (2021). *KEAMANAN SISTEM INFORMASI*.

Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability*. https://doi.org/10.3390/su15129426

Safitri, E. M., Larasati, A. S., & Hari, S. R. (2020). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *JIFTI-Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*. https://doi.org/https://doi.org/10.33005/jifti.v2i1.25

Sahir, S. H. (2021). *METODOLOGI PENELITIAN* (T. Koryati, Ed.; 1st ed.). PENERBIT KBM INDONESIA.

Saleh, T., Kanaan, R., Alzubaidi, R., Kanaan, G. G., & Nino, M. (2025). Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia. *Uncertain Supply Chain Management*, *13*(4), 751–762. https://doi.org/10.5267/j.uscm.2024.12.005

Santyadiputra, G., & Kustono, D. (2023). An Analysis of Cybersecurity Subject and Vilanets Learning Media Towards Vocational School Students' Digital Skills. *Letters in Information Technology Education (LITE)*. https://doi.org/10.17977/um010v6i12023p16-21

Sedgwick, P. (2014). Sample size: How many participants are needed in a cohort study? *BMJ (Online)*, *349*, g6557. https://doi.org/10.1136/bmj.g6557

Sekar. (2024, August 27). *Mengenalkan Cybersecurity dan Etika Digital kepada Siswa*. Https://Almaata.Ac.Id/Mengenalkan-Cybersecurity-Dan-Etika-Digital-Kepada-Siswa/.

Singh, R., & Mangat, N. S. (1996). *Stratified Sampling BT - Elements of Survey Sampling* (R. Singh & N. S. Mangat, Eds.; pp. 102–144). Springer Netherlands. https://doi.org/10.1007/978-94-017-1404-4_5

Singh, R., & Mangat, N. S. (1996). *Stratified Sampling BT - Elements of Survey Sampling* (R. Singh & N. S. Mangat, Eds.; pp. 102–144). Springer Netherlands. https://doi.org/10.1007/978-94-017-1404-4_5

Sudariana, N., & Yoedani, M. M. (2021). *ANALISIS STATISTIK REGRESI LINIER BERGANDA*.

Sugiyono. (2013). *METODE PENELITIAN KUANTITATIF, KUALITATIF, DAN R&D*. ALFABETA, CV.

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information (Switzerland)*, *13*(9). https://doi.org/10.3390/info13090413

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam. *Jurnal Teknologi Dan Informasi*, *14*(2), 163–173. https://doi.org/10.34010/jati.v14i2.12518

Titiakarawongse, C., & Boonkrong, S. (2023). A Study of Password Management Behaviors of Young People. In *Applied Science and Engineering Progress* (Vol. 16, Issue 4). https://doi.org/10.14416/j.asep.2023.01.001

Veronika Asri Tandirerung, Riana T.Mangesa, & Syahrul. (2023). Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. *TEKNOVOKASI : Jurnal Pengabdian Masyarakat*, *1*(2). https://doi.org/https://doi.org/10.59562/teknovokasi.v1i2.131

Walters, M., & Matulich, E. (2009). *Assessing password threats: Implications for formulating university password policies*. https://www.researchgate.net/publication/242779739

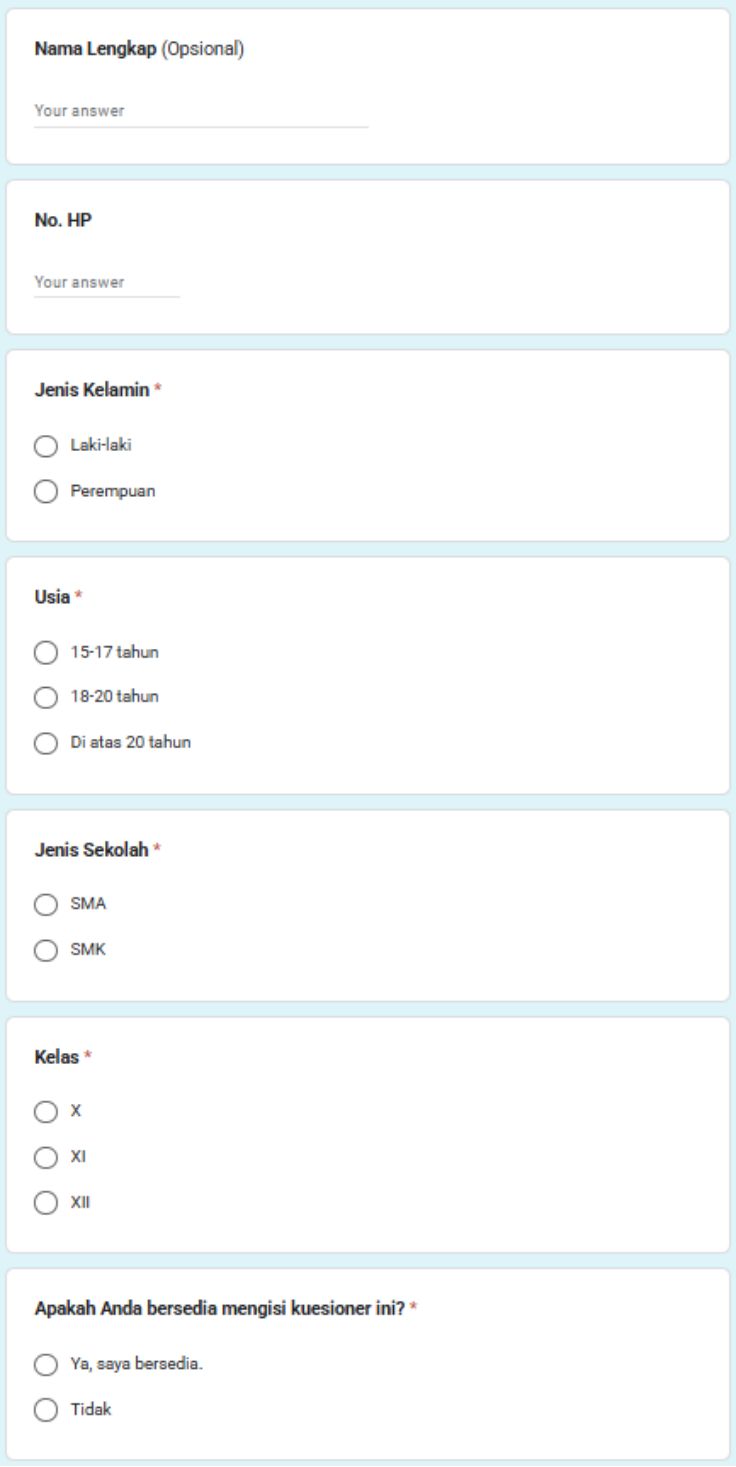
Yanti, H. A. (2021). *PENGOLAHAN DATA SEDERHANA MENGGUNAKAN R STUDIO*.

Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A., & Schaub, F. (2024). Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Transactions on Computer-Human Interaction*, *31*. https://doi.org/10.1145/3689432

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

LAMPIRAN A

Lampiran ini berisi bentuk lengkap kuesioner *Google Forms* yang digunakan untuk mengumpulkan data dari responden. Di dalamnya tercantum seluruh pernyataan yang harus diisi siswa sesuai dengan variabel penelitian. Lampiran ini berfungsi menunjukkan instrumen asli yang diberikan kepada responden.



Nama Lengkap (Opsional)

Your answer

No. HP

Your answer

Jenis Kelamin *

- Laki-laki
- Perempuan

Usia *

- 15-17 tahun
- 18-20 tahun
- Di atas 20 tahun

Jenis Sekolah *

- SMA
- SMK

Kelas *

- X
- XI
- XII

Apakah Anda bersedia mengisi kuesioner ini? *

- Ya, saya bersedia.
- Tidak

Kecemasan Memori

Saya merasa tertekan atau stres ketika harus mengingat banyak kata sandi. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya lebih mudah mengingat kata sandi yang memiliki arti khusus bagi saya (seperti tanggal lahir atau nama panggilan). *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya yakin dapat mengingat kata sandi yang saya buat tanpa perlu menuliskannya. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Seiring bertambahnya usia, saya merasa lebih sulit mengingat kata sandi yang kompleks. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya khawatir lupa kata sandi lama saat membuat kata sandi baru. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Pengaruh Teman Sebaya

Saya akan merasa malu jika teman-teman tahu akun media sosial saya diretas. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Teman-teman akan menganggap saya ceroboh jika akun saya diretas. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya khawatir akan menjadi bahan pembicaraan teman-teman jika akun saya diretas. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya terpengaruh untuk memperbarui perangkat lunak karena teman-teman saya melakukannya. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya termotivasi mencadangkan data penting karena melihat teman-teman melakukannya. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya mengikuti kebijakan keamanan sekolah karena teman-teman saya juga mematuhinya. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Pengalaman Pribadi Keamanan Siber

Saya rutin memeriksa pengaturan privasi di akun media sosial saya. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya selalu memastikan anti-virus di perangkat saya terbaru. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya segera waspada jika perangkat saya berperilaku tidak normal. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya menghindari membuka email dari pengirim tidak dikenal. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya tidak pernah membagikan informasi pribadi di media sosial. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya berhati-hati dengan tautan pendek yang tidak jelas di media sosial. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Persepsi Risiko

Saya merasa akun saya aman dan tidak mungkin diretas. *

	1	2	3	4	5	
Sangat Setuju	○	○	○	○	○	Sangat Tidak Setuju

Saya khawatir data pembayaran game online saya bisa dicuri. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya sadar perangkat saya bisa terinfeksi malware saat bermain game online. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya khawatir transaksi online saya tidak aman. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya menyadari risiko terpengaruh berita palsu di media sosial. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Perilaku Keamanan Kata Sandi

Saya menggunakan kata sandi yang berbeda untuk akun sekolah dan media sosial. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya tidak pernah membagi kata sandi akun sekolah dengan teman. *

	1	2	3	4	5	
Sangat Setuju	○	○	○	○	○	Sangat Tidak Setuju

Saya menggunakan kombinasi huruf, angka, dan simbol dalam kata sandi. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya selalu mengunci perangkat saya saat meninggalkannya. *

	1	2	3	4	5	
Sangat Setuju	○	○	○	○	○	Sangat Tidak Setuju

Saya selalu menghindari mengklik tautan mencurigakan dalam email. *

	1	2	3	4	5	
Sangat Tidak Setuju	○	○	○	○	○	Sangat Setuju

Saya sering mengklik tautan yang ada di email yang dikirim oleh orang yang tidak saya kenal. *

	1	2	3	4	5	
Sangat Setuju	○	○	○	○	○	Sangat Tidak Setuju

LAMPIRAN B

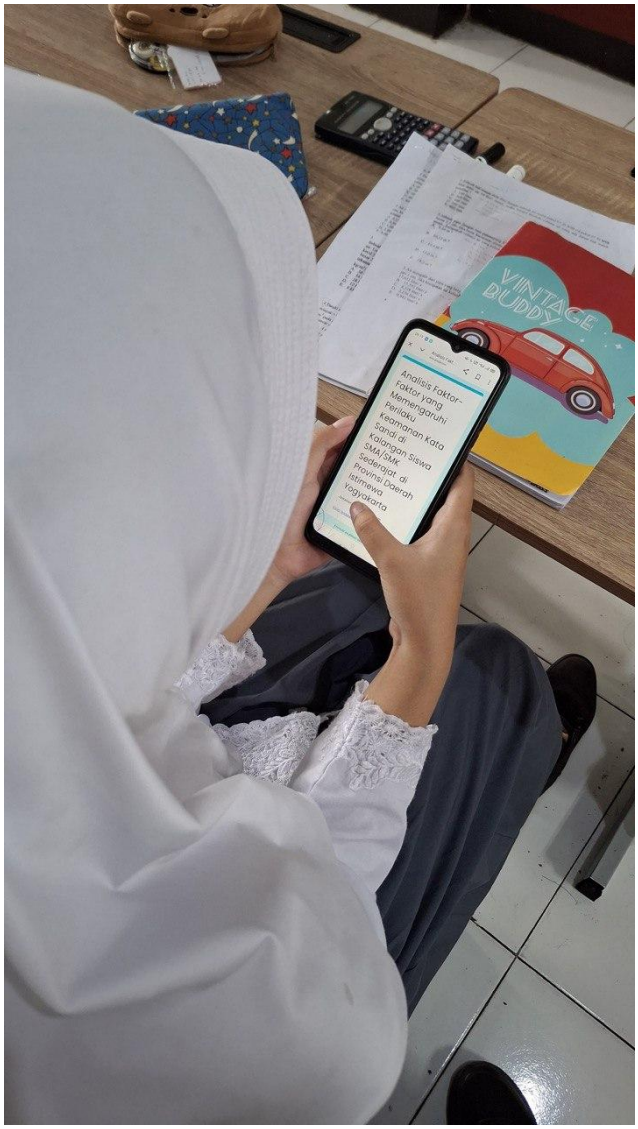
Lampiran ini menyajikan kuesioner dalam format tabel yang terdiri dari nama variabel, kode item, pernyataan, indikator pengukuran, serta sumber rujukan teorinya. Lampiran ini digunakan untuk menunjukkan dasar konseptual dari setiap item pernyataan dan memastikan bahwa instrumen penelitian tersusun secara sistematis dan dapat dipertanggungjawabkan.

Variabel	Kode	Pernyataan	Indikator & Sumber
Kecemasan Ingatan	KI1	Saya merasa tertekan atau stres ketika harus mengingat banyak kata sandi.	Upaya Mental untuk Mengingat Kata Sandi (Woods and Siponen, 2018)
	KI2	Saya lebih mudah mengingat kata sandi yang memiliki arti khusus bagi saya (seperti tanggal lahir atau nama panggilan)	Kemudahan Mengingat Kata Sandi yang Bermakna (Woods and Siponen, 2018)
	KI3	Saya yakin dapat mengingat kata sandi yang saya buat tanpa perlu menuliskannya	Keyakinan pada Kemampuan Mengingat Kata Sandi (Woods and Siponen, 2018)
	KI4	Seiring bertambahnya usia, saya merasa lebih sulit mengingat kata sandi yang kompleks	Pengaruh Usia terhadap Kemampuan Mengingat Kata Sandi (Woods and Siponen, 2018)
	KI5	Saya khawatir lupa kata sandi lama saat membuat kata sandi baru	Kecemasan terhadap Penggunaan Kata Sandi Lama (Woods and Siponen, 2018)
Pengaruh Teman Sebaya	PTS1	Saya akan merasa malu jika teman-teman tahu akun media sosial saya diretas	Pengaruh Teman terhadap Perasaan Malu jika Akun Diretas (Brown, 2004; Mwagwabi & Jiow, 2021)
	PTS2	Teman-teman akan menganggap saya ceroboh jika akun saya diretas	Persepsi Teman terhadap Kelemahan jika Akun Diretas (Brown, 2004; Mwagwabi & Jiow, 2021)
	PTS3	Saya khawatir akan menjadi bahan pembicaraan teman-teman jika akun saya diretas	Kekhawatiran tentang Gosip dari Teman jika Akun Diretas (Brown, 2004; Mwagwabi & Jiow, 2021)
	PTS4	Saya terpengaruh untuk memperbarui perangkat lunak karena teman-teman saya melakukannya	Teman-teman saya di sekolah secara rutin memperbarui perangkat lunak (Herath & Rao, 2009)
	PTS5	Saya termotivasi mencadangkan data penting karena melihat teman-teman melakukannya	Teman-teman mencadangkan data penting mereka (Herath & Rao, 2009)
	PTS6	Saya mengikuti kebijakan keamanan sekolah karena teman-teman saya juga mematuhinya	Teman-teman mematuhi kebijakan keamanan sekolah (Herath & Rao, 2009)
Pengalaman Keamanan Siber Pribadi	PKSP1	Saya rutin memeriksa pengaturan privasi di akun media sosial saya	Saya secara rutin meninjau pengaturan privasi (Shih et al., 2008)
	PKSP2	Saya selalu memastikan anti-virus di perangkat saya terbaru	Saya menjaga perangkat lunak anti-virus tetap diperbarui (Davinson & Sillence, 2010)
	PKSP3	Saya segera waspada jika perangkat saya berperilaku tidak normal	Saya selalu waspada terhadap perilaku perangkat yang tidak biasa (Ng et al., 2009)
	PKSP4	Saya menghindari membuka email dari pengirim tidak dikenal	Saya tidak membuka lampiran email dari pengirim yang tidak dikenal (Anwar et al., 2016)
	PKSP5	Saya tidak pernah membagikan informasi pribadi di media sosial	Saya tidak pernah membagikan informasi pribadi (Anwar et al., 2016)
	PKSP6	Saya berhati-hati dengan tautan pendek yang tidak jelas di media sosial	Saya tidak mengklik tautan pendek yang tidak jelas (Anwar et al., 2016)
Persepsi Risiko	PR1	Saya merasa akun saya aman dan tidak mungkin diretas *	Risiko penipuan atau peretasan akun (*reverse coded) (Brende et al., 2022)
	PR2	Saya khawatir data pembayaran game online saya bisa dicuri	Risiko pencurian akun atau data pembayaran (Brende et al., 2022)
	PR3	Saya sadar perangkat saya bisa terinfeksi malware saat bermain game online	Risiko malware melalui platform gaming (Brende et al., 2022)
	PR4	Saya khawatir transaksi online saya tidak aman	Risiko transaksi yang tidak aman (Brende et al., 2022)
	PR5	Saya menyadari risiko terpengaruh berita palsu di media sosial	Risiko terpapar berita palsu (Brende et al., 2022)
Perilaku Keamanan Kata Sandi	PKKS1	Saya menggunakan kata sandi yang berbeda untuk akun sekolah dan media sosial	Penggunaan Kata Sandi yang Berbeda (Witsenboer et al., 2022)
	PKKS2	Saya tidak pernah membagi kata sandi akun sekolah dengan teman	Berbagi Kata Sandi Sekolah dengan Teman (*reverse coded) (Witsenboer et al., 2022)
	PKKS3	Saya menggunakan kombinasi huruf, angka, dan simbol dalam kata sandi	Penggunaan Kombinasi Huruf, Angka, dan Simbol (Witsenboer et al., 2022)
	PKKS4	Saya selalu mengunci perangkat saya saat meninggalkannya	Meninggalkan Perangkat Tidak Terkunci (*reverse coded) (Witsenboer et al., 2022)
	PKKS5	Saya selalu menghindari mengklik tautan mencurigakan dalam email	Menghindari Klik Tautan dalam Email Tidak Dikenal (Witsenboer et al., 2022)
	PKKS6	Saya sering mengklik tautan yang ada di email yang dikirim oleh orang yang tidak saya kenal *	Klik Tautan pada Email dari Pengirim Tidak Dikenal (*reverse coded) (Witsenboer et al., 2022)

LAMPIRAN C

Lampiran ini berisi dokumentasi pengambilan sampel secara langsung (luring) di sekolah-sekolah yang menjadi lokasi penelitian.











LAMPIRAN D

Lampiran ini memuat seluruh kode R yang digunakan dalam analisis data, mencakup uji validitas, uji reliabilitas, analisis deskriptif, uji asumsi klasik, serta regresi linier berganda. Penyertaan lampiran ini bertujuan memberikan transparansi proses analisis dan memungkinkan replikasi oleh peneliti lain.

```r
# --- LANGKAH 1: PERSIAPAN ---
install.packages(c("tidyverse", "psych", "lmtest", "car", "readr"))

# Muat library yang dibutuhkan
library(tidyverse)
library(psych)
library(lmtest)
library(car)
library(readr)

# --- LANGKAH 2: MEMBUAT SKOR VARIABEL ---
# Menghitung skor rata-rata untuk setiap variabel penelitian
data$Kecemasan_Ingatan <- rowMeans(data[, c("KI1", "KI2", "KI3", "KI4", "KI5")], na.rm = TRUE)
data$Pengaruh_Teman_Sebaya <- rowMeans(data[, c("PTS1", "PTS2", "PTS3", "PTS4", "PTS5", "PTS6")], na.rm =
TRUE)
data$Pengalaman_Keamanan_Siber_Pribadi <- rowMeans(data[, c("PKSP1", "PKSP2", "PKSP3", "PKSP4", "PKSP5",
"PKSP6")], na.rm = TRUE)
data$Persepsi_Risiko <- rowMeans(data[, c("PR1", "PR2", "PR3", "PR4", "PR5")], na.rm = TRUE)
data$Perilaku_Keamanan_Kata_Sandi <- rowMeans(data[, c("PKKS1", "PKKS2", "PKKS3", "PKKS4", "PKKS5",
"PKKS6")], na.rm = TRUE)


# --- LANGKAH 3: MENJALANKAN SEMUA ANALISIS STATISTIK ---

# 4.1 Analisis Deskriptif
print("--- 4.1 HASIL: ANALISIS DESKRIPTIF ---")
descriptives <- data %>% select(Kecemasan_Ingatan, Pengaruh_Teman_Sebaya,
Pengalaman_Keamanan_Siber_Pribadi, Persepsi_Risiko, Perilaku_Keamanan_Kata_Sandi)
print(describe(descriptives))

# 4.2 Uji Reliabilitas
print("--- 4.2 HASIL: UJI RELIABILITAS (CRONBACH'S ALPHA) ---")
print("Alpha Kecemasan Ingatan (X1):")
print(psych::alpha(data[, c("KI1", "KI2", "KI3", "KI4", "KI5")])$total$raw_alpha)
print("Alpha Pengaruh Teman Sebaya (X2):")
print(psych::alpha(data[, c("PTS1", "PTS2", "PTS3", "PTS4", "PTS5", "PTS6")])$total$raw_alpha)
print("Alpha Pengalaman Keamanan Siber Pribadi (X3):")
print(psych::alpha(data[, c("PKSP1", "PKSP2", "PKSP3", "PKSP4", "PKSP5", "PKSP6")])$total$raw_alpha)
print("Alpha Persepsi Risiko (X4):")
print(psych::alpha(data[, c("PR1", "PR2", "PR3", "PR4", "PR5")])$total$raw_alpha)
print("Alpha Perilaku Keamanan Kata Sandi (Y):")
print(psych::alpha(data[, c("PKKS1", "PKKS2", "PKKS3", "PKKS4", "PKKS5", "PKKS6")])$total$raw_alpha)


# Membuat model regresi dengan 4 variabel independen
model_revised <- lm(Perilaku_Keamanan_Kata_Sandi ~ Kecemasan_Ingatan + Pengaruh_Teman_Sebaya +
Pengalaman_Keamanan_Siber_Pribadi + Persepsi_Risiko, data = data)


# 4.3 Uji Asumsi Klasik
print("--- 4.3 HASIL: UJI ASUMSI KLASIK ---")
# 4.3.1 Uji Normalitas (Kolmogorov-Smirnov)
print(">>> Hasil Uji Normalitas (Kolmogorov-Smirnov) pada Residual:")
residuals_model <- residuals(model_revised)

# Standarisasi residual (agar memiliki mean 0 dan sd 1)
residuals_std <- scale(residuals_model)

# Uji normalitas Kolmogorov-Smirnov terhadap distribusi normal
ks_result <- ks.test(residuals_std, "pnorm")

print(ks_result)

qqnorm(residuals(model_revised),
       main = "Normal Q-Q Plot Residual")
qqline(residuals(model_revised))

# 4.3.2 Uji Linearitas
avPlots(model_revised)

# 4.3.3 Uji Multikolinearitas
print(">>> Hasil Uji Multikolinearitas (VIF):")
print(vif(model_revised))

# 4.3.4 Uji Heteroskedastisitas
print(">>> Hasil Uji Heteroskedastisitas (Breusch-Pagan):")
print(bptest(model_revised))

# 4.4 Analisis Regresi Linier Berganda dan Uji Hipotesis
print("--- 4.4 HASIL: ANALISIS REGRESI LINIER BERGANDA ---")
print(summary(model_revised))
```