

Analisis Tingkat Kesadaran Keamanan Informasi Media Sosial (Instagram, Tiktok, Facebook) Pada Kalangan Gen Z Dengan Umur 18-23 Tahun Di Yogyakarta

**Alexandro Gerardo Moksa¹, Kevin Melvern Nugroho², Laurensius Dimas Anugerah Pratama³,
Dimas Wicaksono Wibowo⁴**

^{1,2,3,4} Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta, Yogyakarta, Indonesia

Article Info	ABSTRAK
Article history: Received Juni 21, 2026 Revised Juni 23, 2026 Accepted Juni 23, 2026 Kata Kunci: Information Security Awareness, Generation Z, Social Media Security Keywords: Information Security Awareness, Generation Z, Social Media Security	Penggunaan internet di kalangan anak muda saat ini sangat tinggi, sejalan dengan meningkatnya ancaman kejahatan siber seperti pencurian data pribadi. Generasi Z banyak menghabiskan waktu di media sosial namun sering mengabaikan pengaturan keamanan dasar karena merasa akunnya aman, sehingga pengukuran tingkat kesadaran keamanan informasi menjadi sangat penting dilakukan. Tujuan penelitian yaitu bertujuan untuk mengetahui tingkat kesadaran Generasi Z dengan usia 18 hingga 23 tahun di Daerah Istimewa Yogyakarta dalam menjaga keamanan data, serta membandingkan kebiasaan mereka saat menggunakan Instagram, TikTok, dan Facebook. Target utamanya adalah memberikan rekomendasi yang jelas mengenai kebiasaan pengguna sebagai bahan edukasi keamanan digital. Penelitian ini menggunakan metode kuantitatif dengan menyebarkan kuisioner dengan beberapa pertanyaan yang dilakukan secara daring. Responden dipilih menggunakan teknik purposive sampling, dan datanya akan diuji untuk melihat perbedaan tingkat kesadaran antar platform. Target luaran, Jurnal Teknologi dan Informasi atau Jurnal Sistem Informasi. Juga berupa dokumen utuh yang disusun secara rapi dan komprehensif. Dokumen lengkap tersebut nantinya akan diserahkan sebagai syarat utama pemenuhan kelulusan akademik mahasiswa. ABSTRACT <i>Internet usage among young people is currently very high, along with the increasing threat of cybercrime such as personal data theft. Generation Z spends a lot of time on social media but often ignores basic security settings because they believe their accounts are secure, making measuring information security awareness very important. The purpose of this study is to determine the level of awareness of Generation Z aged 18 to 23 in the Special Region of Yogyakarta regarding maintaining data security, as well as to compare their habits when using Instagram, TikTok, and Facebook. The main goal is to provide clear recommendations regarding user habits as material for digital security education. This study uses a quantitative method by distributing a questionnaire with several bold questions. Respondents were selected using a purposive sampling technique, and the data will be examined to identify differences in awareness levels between platforms. The target output is the Journal of Technology and Information or the Journal of Information Systems. It is also a complete document that is neatly and comprehensively arranged. The complete document will later be submitted as the main requirement for students' academic graduation.</i> <i>This is an open access article under the CC BY license</i>



Corresponding Author:

Alexandro Gerardo Moksa
Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta,
Yogyakarta, Indonesia
Email: laurensdap@gmail.com

1. PENDAHULUAN

Perkembangan teknologi komunikasi membuat media sosial menjadi tempat utama bagi masyarakat untuk bertukar informasi setiap hari. Perluasan jaringan internet telah mengubah cara orang berinteraksi dan membagikan data pribadi mereka di dunia maya. Kemudahan dalam mengakses informasi ini ternyata membawa risiko besar berupa meningkatnya ancaman keamanan siber. Masalah seperti pencurian identitas, penipuan, dan penyalahgunaan data pribadi kini menjadi ancaman nyata yang butuh penanganan serius. Bentuk ancaman ini sekarang juga makin beragam dan menjebak. Misalnya saja, maraknya link phishing yang disebar melalui pesan langsung berkedok promo menarik, atau tren membagikan riwayat hidup melalui video pendek yang secara tidak sadar mengekspos data pribadi seperti nama keluarga hingga lokasi tempat tinggal. Hal-hal seperti ini sering kali memakan korban justru dari kalangan anak muda yang seharusnya melek teknologi. Kesadaran pengguna dalam menjaga keamanan data menjadi benteng pertahanan pertama untuk menghadapi bahaya tersebut.

Pemahaman yang baik tentang cara kerja keamanan digital sangat menentukan keberhasilan kita dalam mencegah serangan siber. Penerapan kebiasaan aman saat menggunakan internet harus menjadi bagian dari kehidupan sehari-hari setiap orang. Hal ini sangat penting untuk mengurangi risiko hilangnya informasi pribadi yang berharga. Penelitian tentang kesadaran keamanan informasi ini difokuskan pada kelompok Generasi Z yang berusia antara 18 hingga 23 tahun. Kelompok usia ini dipilih karena mereka sudah sangat akrab dengan dunia digital sejak usia dini. Mereka juga menggunakan platform media sosial populer seperti Instagram, TikTok, dan Facebook secara terus-menerus setiap harinya. Ketiga platform tersebut memiliki aturan privasi dan cara penyebaran konten yang berbeda satu sama lain. Instagram berfokus pada foto dan video, TikTok mengandalkan rekomendasi sistem, sedangkan Facebook lebih menitikberatkan pada jaringan pertemanan. Perbedaan fitur ini membuat cara Generasi Z mengatur privasi data mereka menjadi sangat beragam dan menarik untuk diteliti.

Generasi Z di Yogyakarta umumnya memiliki pola kebiasaan yang berbeda saat mengakses ketiga aplikasi ini. Instagram sering digunakan sebagai tempat untuk memajang portofolio atau kegiatan sehari-hari sehingga rawan terhadap penyalahgunaan foto. Di sisi lain, algoritma TikTok yang mendorong pengguna untuk selalu masuk membuat pengguna lengah dan membagikan privasi melalui konten keseharian kehidupan. Sementara itu, Facebook kini lebih sering dimanfaatkan mahasiswa untuk mencari informasi indekos atau melakukan transaksi jual beli di grup terbuka, yang tentunya memiliki celah kerawanan penipuan identitas yang berbeda pula. Wilayah Daerah Istimewa Yogyakarta dipilih sebagai lokasi penelitian karena statusnya sebagai kota pelajar yang diisi oleh mahasiswa dari berbagai daerah. Keberadaan banyak pemuda terdidik di kota ini memberikan gambaran yang pas untuk mengukur tingkat pemahaman keamanan siber secara umum.

Kasus pencurian data pribadi di media sosial terus meningkat dan tercatat dalam berbagai laporan resmi. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia menunjukkan bahwa hampir seluruh kalangan remaja dan dewasa muda sudah terhubung ke internet [1]. Tingginya angka penggunaan internet ini ternyata sejalan dengan banyaknya kasus kebocoran data yang merugikan masyarakat [2]. Laporan keamanan digital tahunan juga mencatat ribuan kasus peretasan akun media sosial yang menargetkan pengguna biasa. Beberapa studi membuktikan bahwa Generasi Z sering membagikan

terlalu banyak informasi pribadi sehingga mereka mudah menjadi korban penipuan [3]. Mereka sering kali malas mengubah pengaturan keamanan pada aplikasi karena merasa akun mereka tidak akan diretas [4]. Berbagai modus penipuan melalui pesan singkat di dalam aplikasi masih sering berhasil mengelabui kalangan yang berpendidikan [5]. Kenyataan bahwa anak muda pandai menggunakan teknologi tetapi kurang peduli pada keamanan dasar menjadi alasan kuat mengapa penelitian ini harus dilakukan.

Banyak penelitian sebelumnya yang telah membahas hubungan antara penggunaan media sosial dan perilaku menjaga keamanan informasi. Cara Generasi Z di Jawa Tengah dan Yogyakarta mengatur privasi mereka agar data tidak disalahgunakan. Mereka menemukan bahwa banyak anak muda peduli pada privasi namun tidak melakukan tindakan pencegahan yang nyata [6]. Mengukur tingkat kesadaran keamanan data mahasiswa khusus pada aplikasi Instagram. Hasilnya menunjukkan bahwa mahasiswa masih memiliki tingkat keamanan menengah dan mudah terkena tipuan [7].

Studi dari Sampe Allo dkk, menggunakan teori motivasi perlindungan untuk melihat bagaimana pengguna media sosial menjaga akun mereka. Penelitian tersebut menegaskan bahwa keyakinan pengguna terhadap kemampuan mereka sendiri sangat memengaruhi tindakan pengamanan data [8]. Ketiga penelitian ini membuktikan bahwa faktor pemahaman pengguna sangat penting untuk memastikan sistem keamanan digital berjalan dengan baik.

Tinjauan terhadap penelitian-penelitian terdahulu menunjukkan adanya beberapa kekurangan yang perlu diperbaiki. Sebagian besar penelitian sebelumnya hanya berfokus pada satu atau dua aplikasi media sosial saja. Belum banyak yang membandingkan tingkat kesadaran keamanan pengguna di tiga aplikasi besar seperti Instagram, TikTok, dan Facebook sekaligus. Rentang usia yang diteliti pada penelitian sebelumnya juga sering kali terlalu luas sehingga tidak menggambarkan kebiasaan kelompok usia 18 hingga 23 tahun secara khusus. Lokasi penelitian yang dilakukan juga jarang menyoroti Yogyakarta sebagai kota pelajar yang memiliki perputaran informasi digital sangat cepat.

Ketiadaan penelitian yang menggabungkan ketiga aplikasi tersebut membuat kita belum memiliki gambaran utuh tentang kebiasaan aman pengguna. Kekurangan inilah yang menjadi alasan kuat untuk membuat penelitian baru yang lebih menyeluruh. Penelitian ini hadir untuk melengkapi kekurangan tersebut dengan mengukur kesadaran keamanan berdasarkan jenis platform, usia, dan lokasi secara spesifik. Berbagai alasan tersebut mendorong penelitian ini untuk mencari tahu seberapa sadar Generasi Z di Yogyakarta terhadap keamanan informasi. Penelitian ini ingin melihat perbedaan tingkat kesadaran pengguna dalam mengamankan data pribadi mereka di Instagram, TikTok, dan Facebook.

2. METODE

3.1 Variabel Penelitian dan Definisi Operasional

Untuk menghindari terjadinya kerancuan interpretasi dan ambiguitas selama proses pengumpulan serta pengolahan data di lapangan, seluruh komponen yang dikaji dalam penelitian ini diklasifikasikan ke dalam variabel yang tertata. Variabel utama yang diamati secara mendalam meliputi tingkat kesadaran keamanan informasi yang diposisikan sebagai variabel terikat, serta jenis platform media sosial (Instagram, TikTok, dan Facebook) yang bertindak sebagai variabel bebas atau faktor pembanding.

Untuk mengukur variabel terikat tersebut, penelitian ini menggunakan instrumen Human Aspects of Information Security Questionnaire (HAIS-Q). Penggunaan instrumen HAIS-Q didasarkan pada kemampuan model tersebut untuk mengukur aspek perilaku manusia terkait keamanan informasi secara spesifik. HAIS-Q dirancang untuk mengevaluasi kebiasaan, tindakan nyata, dan pemahaman operasional pengguna yang sudah aktif menggunakan platform informasi. Karena Generasi Z telah terbukti mengadopsi media sosial secara masif, fokus penelitian bergeser pada dimensi perilaku aman (behavioral security), sehingga dimensi dalam HAIS-Q menjadi instrumen yang tepat untuk membahas penelitian ini.

3.2 Teknik Pengumpulan Data dan Sampel

Subbab ini menguraikan langkah-langkah strategis yang digunakan oleh peneliti untuk memperoleh data primer dari lapangan. Pembahasan di dalamnya mencakup penentuan kriteria spesifik yang harus dipenuhi oleh responden, perhitungan matematis untuk menentukan batas minimal ukuran sampel yang representatif, serta teknis pelaksanaan distribusi instrumen penelitian.

3.2.1 Kriteria Sampel (Purposive Sampling)

Proses pengambilan sampel di lapangan dilakukan menggunakan teknik nonprobabilitas dengan metode purposive sampling. Penggunaan teknik ini mengharuskan setiap responden yang dipilih memenuhi kriteria inklusi khusus yang telah ditetapkan sebelumnya oleh peneliti. Hal ini bertujuan agar data yang diperoleh benar-benar terarah, relevan, dan akurat sesuai ruang lingkup penelitian. Syarat wajib yang harus dipenuhi oleh responden meliputi: berusia antara 18 hingga 23 tahun (mewakili kelompok rentang usia Generasi Z secara spesifik), benar-benar berdomisili di wilayah Daerah Istimewa Yogyakarta, serta aktif menggunakan minimal satu dari ketiga media sosial utama yang diteliti, yaitu Instagram, TikTok, atau Facebook.

3.2.2 Penentuan Ukuran Sampel

Populasi dalam penelitian ini adalah kelompok Generasi Z yang berusia antara 18 hingga 23 tahun dan berdomisili di wilayah Daerah Istimewa Yogyakarta. Mengingat jumlah populasi riil secara makro sangat besar dan dinamis, penentuan ukuran sampel minimum yang representatif dihitung menggunakan Rumus Slovin. Untuk menyesuaikan dengan ruang lingkup, efisiensi kerja lapangan, dan keterbatasan durasi waktu penelitian kuantitatif ini, tingkat toleransi kesalahan (margin of error) ditetapkan pada angka 10% (0,1).

Dalam menentukan nilai total populasi (N), peneliti melakukan pendekatan proporsional berdasarkan data proyeksi kependudukan terbaru dari Badan Pusat Statistik (BPS) Provinsi Daerah Istimewa Yogyakarta. Berdasarkan data agregat BPS, total populasi pemuda pada kelompok umur 15–24 tahun di DIY tercatat berada di kisaran 610.000 jiwa. Karena pengelompokan usia berkala BPS menggunakan rentang per 5 tahun, maka nilai N untuk sub kelompok usia 18–23 tahun (yang mencakup 6 tahun dari total 10 tahun rentang kategori BPS tersebut) dihitung menggunakan pendekatan proporsi persentase sebesar 60% dari total populasi pemuda. Melalui kalkulasi matematis tersebut ($60\% \times 610.000$), diperoleh angka estimasi populasi target sebesar 366.000 jiwa, yang kemudian dikenakan secara konservatif menjadi 350.000 jiwa untuk kebutuhan perhitungan sampel.

Berdasarkan nilai parameter kependudukan tersebut, proses perhitungan ukuran sampel diuraikan sebagai berikut :

$$\begin{aligned} n &= \frac{350.000}{1 + 350.000 * (0,1)^2} \\ n &= \frac{350.000}{1 + 350.000 * 0,01} \\ n &= \frac{350.000}{1 + 3.500} \\ n &= \frac{350.000}{3.501} \\ n &= 99,97 \end{aligned}$$

Berdasarkan hasil kalkulasi matematis menggunakan rumus Slovin di atas, diperoleh nilai akhir sebesar 99,97. Berdasarkan kaidah statistik inferensial untuk pembulatan ukuran sampel manusia ke atas, maka jumlah sampel minimal yang wajib dikumpulkan dalam penelitian lapangan ini ditetapkan menjadi genap 100 responden. Target 100 sampel ini dinilai sudah memenuhi ambang batas keterwakilan populasi berskala besar, sekaligus menjaga keseimbangan sebaran data untuk pengujian hipotesis komparatif menggunakan ANOVA pada tiap kelompok platform media sosial (Instagram, TikTok, dan Facebook) yang diteliti. Pengumpulan data terhadap seratus sampel tersebut akan dilaksanakan melalui penyebaran kuesioner secara daring menggunakan platform formulir elektronik yang disebarluaskan secara terarah ke berbagai jaringan mahasiswa di Yogyakarta.

3.3 Analisis Data

Setelah data lapangan berhasil terkumpul sesuai dengan batas minimal sampel yang telah ditetapkan, tahap analisis data akan dihitung secara komputerisasi menggunakan perangkat lunak statistik seperti SPSS. Proses analisis ini menerapkan metode uji beda komparatif untuk membuktikan hipotesis kelompok. Pengujian statistik ini memiliki tujuan utama yang sangat krusial, yaitu untuk memastikan apakah perbedaan skor tingkat kesadaran di antara pengguna ketiga platform tersebut benar-benar nyata dan signifikan secara statistik, atau hanya terjadi secara kebetulan semata akibat variasi data minor di lapangan.

Rincian tahapan analisis data kuantitatif yang akan dilakukan meliputi:

1. **Pembersihan Data (Data Cleaning)** : Data mentah yang masuk dari pengisian kuesioner daring tidak bisa langsung diuji. Peneliti akan melakukan seleksi awal untuk mendeteksi dan membuang respons data yang tidak valid, mengandung jawaban ganda, kuesioner yang tidak lengkap, atau data yang dikirimkan oleh responden yang ternyata berada di luar kriteria inklusi usia serta lokasi.
2. **Analisis Deskriptif** : Tahapan ini dilakukan untuk mendeskripsikan karakteristik profil responden secara umum (seperti distribusi usia dan jenis kelamin) serta menyajikan nilai rata-rata (mean), nilai tengah (median), nilai minimum, nilai maksimum, dan standar deviasi dari skor kesadaran keamanan pada masing-masing kelompok platform media sosial.
3. **Uji Prasyarat Analisis** : Sebagai syarat wajib sebelum mengeksekusi uji ANOVA yang termasuk ke dalam rumpun statistik parametrik, data skor tingkat kesadaran harus dipastikan memenuhi asumsi dasar statistik. Uji Normalitas akan dilakukan menggunakan metode Kolmogorov Smirnov atau Shapiro Wilk untuk melihat apakah sebaran skor data berdistribusi normal, sedangkan Uji Homogenitas akan dinilai menggunakan Levene's Test untuk memastikan varians data di antara ketiga kelompok pengguna platform bersifat sama atau homogen.
4. **Uji Hipotesis Komparatif (One-Way ANOVA)** : Pengujian utama ini dilakukan untuk menjawab rumusan masalah mengenai perbedaan tingkat kesadaran antar pengguna Instagram, TikTok, dan Facebook. Apabila hasil perhitungan ANOVA menunjukkan nilai probabilitas signifikansi kurang dari 0,05 ($p < 0,05$), maka hipotesis penelitian diterima, yang berarti terbukti secara empiris terdapat perbedaan skor tingkat kesadaran yang nyata dan signifikan. Analisis lanjutan berupa uji PostHoc (seperti Tukey HSD) kemudian akan diaplikasikan untuk membandingkan antar kelompok secara spesifik guna mencari tahu platform mana yang penggunaannya memiliki tingkat kepedulian paling tinggi dan paling rendah terhadap perlindungan data pribadi.

3. HASIL DAN PEMBAHASAN

3.1 Uji Validitas dan Reliabilitas Instrumen

Sebelum dilakukan pengujian hipotesis komparatif, seluruh butir pernyataan instrumen (Item 1 hingga Item 16) yang mengukur tingkat kesadaran keamanan informasi diuji validitas dan reliabilitasnya.

1. **Uji Validitas**: Berdasarkan hasil analisis korelasi *Pearson Product Moment*, seluruh item

(Item 1 sampai Item 16) memiliki nilai signifikansi korelasi terhadap skor total sebesar $p = 0.000$ ($p < 0.05$). Dengan demikian, seluruh butir instrumen dinyatakan valid dan layak digunakan untuk mengukur tingkat kesadaran keamanan informasi responden.

2. Uji Reliabilitas: Pengujian reliabilitas internal instrumen dilakukan dengan melihat nilai *Cronbach's Alpha* dari ke-16 item tersebut.

Tabel 1. Hasil Uji Reliabilitas Instrumen
Reliability Statistics

Cronbach's Alpha	N of Items
.876	16

ONEWAY Total_Skor BY Platform
/STATISTICS DESCRIPTIVES HOMOGENEITY
/MISSING ANALYSIS.

Berdasarkan Tabel 1, nilai *Cronbach's Alpha* yang diperoleh adalah 0.876. Karena nilai ini jauh melampaui batas ambang batas minimum statistik kualifikasi reliabilitas ($\alpha > 0.60$ atau 0.70), maka instrumen penelitian ini dinyatakan sangat reliabel dan memiliki konsistensi internal yang kokoh.

3.2 Analisis Statistik Deskriptif Skor Kesadaran per Platform

Analisis deskriptif dilakukan untuk memetakan capaian nilai rata-rata (*mean*), standar deviasi, nilai minimum, dan nilai maksimum dari total skor kesadaran keamanan informasi pada tiap kelompok media sosial.

Tabel 2. Nilai Deskriptif Total Skor Kesadaran Keamanan Informasi

Descriptives						
Total_Skor						
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
Instagram	36	63.9722	9.79938	1.63323	60.6566	67.2879
Tiktok	31	67.2581	6.09354	1.09443	65.0229	69.4932
Facebook	41	64.7561	10.91279	1.70429	61.3116	68.2006
Total	108	65.2130	9.38885	.90344	63.4220	67.0039

Descriptives		
Total_Skor		
	Minimum	Maximum
Instagram	26.00	80.00
Tiktok	48.00	80.00
Facebook	25.00	79.00
Total	25.00	80.00

Berdasarkan Tabel 2, sebaran jumlah responden (N) relatif berimbang dengan sampel pengguna Facebook paling banyak (41 responden) diikuti Instagram (36 responden) dan TikTok (31 responden). Secara deskriptif, pengguna TikTok memiliki nilai rata-rata kesadaran tertinggi sebesar 67.2581 dengan variasi jawaban terkecil (*Std. Deviation* = 6.09354). Sementara itu, pengguna Instagram menunjukkan

rata-rata kesadaran terendah sebesar 63.9722. Dengan rentang nilai ekstrem bawah ditemukan pada pengguna Facebook (Min = 25.00) dan Instagram (Min = 26.00).

3.3 Uji Prasyarat Analisis (Normalitas dan Homogenitas)

Sebagai dasar penggunaan statistik parametrik *One-Way ANOVA*, data harus memenuhi uji asumsi klasik.

3.3.1 Uji Normalitas: Pengujian sebaran distribusi data dilakukan dengan uji *Kolmogorov-Smirnov* dan *Shapiro-Wilk*.

Tabel 3. Hasil Uji Normalitas Sebaran Data

Tests of Normality						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Total_Skor	.219	108	.000	.761	108	.000

a. Lilliefors Significance Correction

Hasil uji pada Tabel 3 menunjukkan nilai signifikansi sebesar 0.000 ($p < 0.05$). Hal ini mengindikasikan bahwa secara matematis sebaran data total skor tidak berdistribusi normal. Kondisi ini dipengaruhi oleh tingginya kemiringan data (*Skewness* = -2.253) dan keruncingan (*Kurtosis* = 6.943), di mana mayoritas responden cenderung mengelompok pada skor tinggi (*ceiling effect*), namun terdapat segelintir pencilan ekstrem di batas bawah. Meskipun demikian, uji ANOVA tetap dapat dilanjutkan karena jumlah sampel total ($N = 108$) cukup besar dan mengacu pada teorema limit pusat yang memitigasi pelanggaran minor normalitas.

3.3.2 Uji Homogenitas: Pengujian kesamaan varians antar kelompok diuji menggunakan *Levene's Test*.

Tabel 4. Hasil Uji Homogenitas Varians (Levene's Test)

Test of Homogeneity of Variances					
		Levene Statistic	df1	df2	Sig.
Total_Skor	Based on Mean	2.402	2	105	.096
	Based on Median	1.553	2	105	.216
	Based on Median and with adjusted df	1.553	2	87.352	.217
	Based on trimmed mean	1.937	2	105	.149

Berdasarkan Tabel 4, nilai signifikansi *Levene's Test* berbasis nilai rata-rata (*Based on Mean*) menunjukkan angka 0.096. Karena nilai $p = 0.096 > 0.05$, maka asumsi homogenitas varians antar ketiga platform media sosial dinyatakan terpenuhi atau varians data adalah sama.

3.4 Pengujian Hipotesis Utama (Uji One-Way ANOVA)

Untuk membuktikan apakah terdapat perbedaan tingkat kesadaran keamanan informasi yang signifikan secara statistik di antara pengguna Instagram, TikTok, dan Facebook, maka dilakukan analisis *One-Way ANOVA*.

Tabel 5. Hasil Analisis One-Way ANOVA

ANOVA

Total_Skor

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	193.633	2	96.817	1.100	.337
Within Groups	9238.469	105	87.985		
Total	9432.102	107			

```

EXAMINE VARIABLES=Total_Skor
/PLOT BOXPLOT STEMLEAF NPLOT
/COMPARE GROUPS
/STATISTICS DESCRIPTIVES
/CINTERVAL 95
/MISSING LISTWISE
/NOTOTAL.

```

Berdasarkan Tabel 5, nilai *F-hitung* yang diperoleh adalah 1.100 dengan nilai probabilitas signifikansi sebesar 0.337. Karena nilai signifikansi $0.337 > 0.05$, maka keputusan statistik yang diambil adalah gagal menolak H_0 dan menolak H_1 . Hal ini membuktikan secara empiris bahwa tidak terdapat perbedaan tingkat kesadaran keamanan informasi yang signifikan antara Generasi Z pengguna Instagram, TikTok, maupun Facebook di Yogyakarta. Oleh karena hasil ANOVA tidak signifikan, maka pengujian lanjutan berupa *Post-Hoc Tukey HSD* tidak perlu dilakukan.

3.5 Pembahasan

Hasil pengolahan data mengungkap fakta menarik yang justru menolak hipotesis awal penelitian ini. Jika dilihat secara deskriptif, kelompok pengguna TikTok memang mencatatkan rata-rata skor kesadaran tertinggi (67.25), disusul oleh Facebook (64.75) dan Instagram (63.97). Kendati demikian, selisih angka tersebut ternyata tidak cukup besar untuk dikatakan signifikan secara statistik. Fenomena ini dapat dijelaskan melalui beberapa sudut pandang berikut.

3.5.1 Interpretasi Kesadaran Keamanan Berdasarkan HAIS-Q

Berdasarkan pengukuran menggunakan instrumen HAIS-Q yang mencakup dimensi manajemen kata sandi, pengamanan akun (2FA), privasi profil, dan eksposur data diperoleh rata-rata skor gabungan sebesar 65.21 dari total 80 poin. Capaian ini mengindikasikan bahwa secara kognitif maupun sikap, mahasiswa Generasi Z di Yogyakarta sudah memiliki pemahaman keamanan siber di level menengah ke atas.

Tingkat pemahaman yang relatif baik ini ternyata membentuk pola perilaku yang seragam (*homogen*) saat mereka menggunakan media sosial. Setiap platform sebenarnya memiliki karakteristik kerawanan masing-masing: Instagram dengan eksposur visualnya, TikTok yang algoritma FYP-nya sering memancing *oversharing*, dan Facebook dengan grup terbukanya yang rawan praktik *phishing*. Namun, perbedaan kerawanan struktural dari ketiga aplikasi tersebut terbukti tidak mengubah standar perlindungan diri yang diterapkan oleh para penggunanya.

3.5.2 Homogenitas Perilaku Lintas Platform Generasi Z

Ditolaknya hipotesis perbedaan kesadaran antarplatform ini sangat sejalan dengan karakteristik bawaan Generasi Z. Sebagai kelompok *digital native* yang lahir di era internet, mereka melihat berbagai aplikasi media sosial bukan sebagai hal yang terpisah, melainkan sebuah ekosistem lintas platform (*cross-platform*) yang diakses secara bersamaan setiap harinya. Oleh karena itu, standar keamanan yang mereka terapkan seperti menjaga kerahasiaan kata sandi atau mengatur privasi akun telah mengakar menjadi pola kebiasaan dasar (*behavior*). Kebiasaan aman ini akan terus mereka bawa tanpa

memedulikan aplikasi apa yang sedang mereka operasikan.

3.5.3 Perbandingan dengan Penelitian Terdahulu (State of the Art)

Temuan dalam penelitian ini sekaligus mengisi celah (*gap*) dari literatur-literatur rujukan sebelumnya:

1. Penelitian ini memperkuat temuan Wasisto Aji (2022) yang menyatakan bahwa manajemen privasi anak muda didorong oleh pemahaman mereka tentang komersialisasi data. Hasil penelitian ini membuktikan bahwa kepedulian privasi tersebut bersifat kolektif dan tidak terkotak-kotak pada satu platform saja.
2. Studi Al Gazali dkk. (2025) sebelumnya menyimpulkan bahwa tingkat kesadaran pengguna Instagram berada di level menengah. Penelitian ini berhasil memperluas temuan tersebut dengan membuktikan bahwa level kesadaran menengah ini rupanya bersifat statis dan setara, bahkan ketika dibandingkan secara langsung dengan pengguna TikTok dan Facebook.
3. Jika dikaitkan dengan *Protection Motivation Theory* dari Sampe Allo dkk., tidak adanya perbedaan skor antarplatform dalam penelitian ini menegaskan satu hal penting: dorongan untuk mengamankan data murni berasal dari keyakinan kemampuan diri (*self-efficacy*) masing-masing individu, bukan dorongan situasional yang dipancing oleh fitur keamanan bawaan dari aplikasinya.

3.5.4 Keterbatasan Penelitian

Kendati penelitian ini telah dilaksanakan secara objektif, peneliti menyadari masih terdapat beberapa keterbatasan teknis maupun metodologis yang berpotensi memengaruhi hasil akhir:

1. Asumsi Normalitas Data Tidak Terpenuhi secara Sempurna Hasil uji statistik menunjukkan sebaran data mengalami kemiringan negatif (*negative skewness*) yang cukup tajam. Artinya, mayoritas responden mengelompok pada pilihan jawaban berskor tinggi (merasa sudah sangat sadar keamanan). Hal ini kemungkinan besar terjadi karena lokasi penelitian berada di Yogyakarta yang notabene adalah kota pelajar. Dominasi individu terdidik dalam sampel penelitian membuat data memiliki bias literasi yang tinggi, sehingga variasi jawaban responden menjadi kurang beragam.
2. Keterbatasan Metode Kuesioner Lapor Mandiri (*Self-Reported Questionnaire*) Pengumpulan data menggunakan kuesioner daring sangat bergantung pada kejujuran dan penilaian subjektif responden (*self-assessment*). Kelemahan utama metode ini adalah rentannya bias *social desirability*, yaitu kecenderungan responden untuk memilih jawaban yang terkesan "paling benar atau ideal" agar terlihat baik secara sosial. Pada kenyataannya, apa yang mereka isi di kuesioner bisa saja berbeda dengan perilaku aslinya sehari-hari, di mana mereka mungkin masih sering membagikan data pribadi secara berlebihan (*oversharing*) karena terjebak pada ilusi rasa aman (*illusion of security*) saat berselancar di internet.

4. KESIMPULAN

Penelitian ini menyimpulkan bahwa tingkat kesadaran keamanan informasi pada Generasi Z berusia 18 hingga 23 tahun di Yogyakarta secara umum sudah berada pada level menengah ke atas. Berdasarkan pengukuran menggunakan instrumen HAIS-Q, para responden mencatatkan rata-rata skor gabungan sebesar 65,21 dari total 80 poin. Meskipun capaian pemahaman ini terbilang baik, hasil pengujian statistik secara komparatif menggunakan *One-Way ANOVA* menunjukkan fakta yang cukup menarik, yaitu tidak ditemukannya perbedaan tingkat kesadaran yang signifikan antara pengguna Instagram, TikTok, maupun Facebook. Ketiadaan perbedaan ini membuktikan secara empiris bahwa

Generasi Z memiliki pola perilaku keamanan siber yang seragam saat berselancar di dunia maya. Praktik perlindungan data pribadi, seperti rutinitas mengganti kata sandi atau mengatur privasi profil, ternyata lebih banyak didorong oleh kebiasaan dasar dan keyakinan diri masing-masing individu, alih-alih dipengaruhi oleh seberapa rawan atau berbedanya fitur keamanan dari aplikasi yang sedang mereka buka.

REFERENSI

- [1] R. A. Syahputra et al., “Informasi Artikel Abstrak,” *Jurnal Pengabdian Kepada Masyarakat Nusantara*, vol. 5, no. 3, pp. 3164–3171, 2024, doi: 10.55338/jpkmn.v5i3.3543.
- [2] A. Sahfitri, “Penipuan Digital Melalui Tautan Phishing,” *Jurnal Dialektika Hukum*, vol. 6, no. 2, 2024. [Online]. Available: <https://bankjombang.co.id/serangan-phishing-di-indonesia-terus>. [Accessed: Aug. 2026].
- [3] N. M. Irwan and P. N. Nasution, “Kesadaran dan Sikap Pengguna terhadap Privasi Data dalam Penggunaan Aplikasi Sosial Media TikTok: Studi Kasus Generasi Z,” *Jurnal Informatika Nusantara*, vol. 1, no. 4, 2024, doi: 10.61722/jinu.v1i4.1886.
- [4] M. A. Rasyidin, A. Putri, M. D. Lestari, R. Nurnajmah, and D. A. Safaraz, “Analisis Kesadaran Mahasiswa dalam Menjaga Keamanan Data Pribadi pada Penggunaan Media,” *Jurnal Teknik Informatika dan Teknologi Informasi*, vol. 5, no. 3, pp. 752–761, Dec. 2025, doi: 10.55606/jutiti.v5i3.6583.
- [5] N. Azmi et al., “Literasi Generasi Z Mengenai Kejahatan Cybercrime di Media Sosial,” *Jurnal Sistem Informasi, Akuntansi dan Manajemen*, vol. 5, no. 3, 2025.
- [6] P. Wasisto Aji and P. Utari, “Manajemen Privasi Generasi Z dalam Menghadapi Komersialisasi Data Pribadi di Media Sosial,” *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, vol. 24, no. 2, pp. 103–116, 2022, doi: 10.17933/iptekkom.24.2.2022.103-116.
- [7] B. K. A. S. Al Gazali, R. B. Huwae, and A. Zubaidi, “Pengukuran Tingkat Kesadaran Keamanan Data Pribadi Mahasiswa Universitas Mataram pada Instagram Menggunakan Metode HAIS-Q,” *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 10, no. 4, pp. 3740–3748, Nov. 2025, doi: 10.29100/jupi.v10i4.9339.
- [8] J. S. Allo, F. S. Rahayu, G. L. Pritalia, E. Pranisti, and J. Marcelino, “Analisis Motivasi Gen Z dalam Menjaga Keamanan Data Pribadi di Media Sosial Menggunakan Protection Motivation Theory (PMT).”