



**BADAN SIBER
DAN SANDI
NEGARA**

2024

SURVEI KESADARAN KEAMANAN SIBER



DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI

www.bssn.go.id



**BADAN SIBER
DAN SANDI
NEGARA**

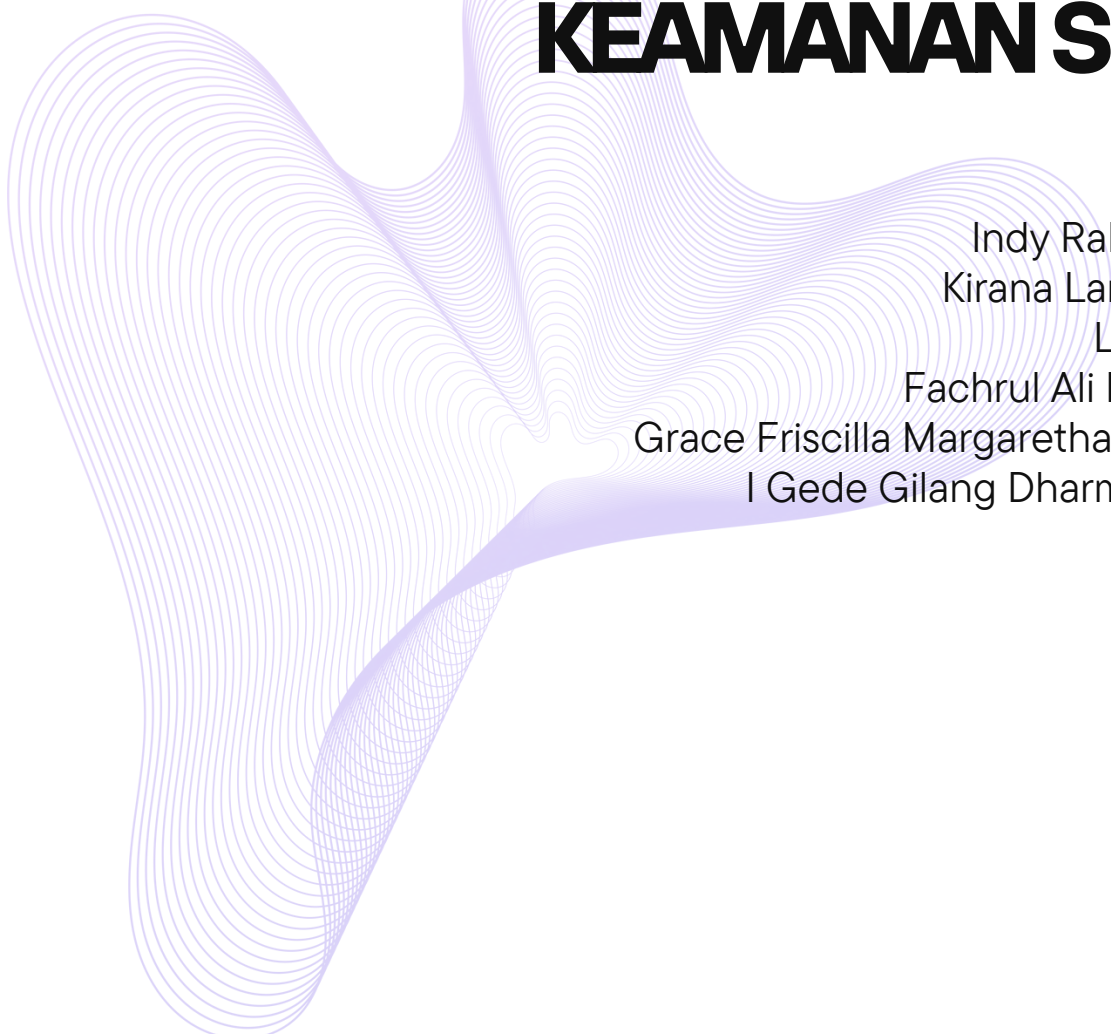
2024

SURVEI KESADARAN KEAMANAN SIBER



DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI

www.bssn.go.id



SURVEI KESADARAN KEAMANAN SIBER

PENULIS

Indy Rahmadhona
Kirana Larasati Dewi

Lisa Saputri

Fachrul Ali Nurfadillah

Grace Friscilla Margaretha Karo-Karo

I Gede Gilang Dharma Suputra

SURVEI KESADARAN KEAMANAN SIBER

PENULIS

Indy Rahmadhona
Kirana Larasati Dewi
Lisa Saputri
Fachrul Ali Nurfadillah
Grace Friscilla Margaretha Karo-Karo
I Gede Gilang Dharma Suputra

PENGARAH

Dominggus Pakel

PENANGGUNG JAWAB

Satryo Suryantoro

KOORDINATOR

Eri Suprayitno

DESAINER GRAFIK, SAMPUL, DAN TATA LETAK

Fachrul Ali Nurfadillah
Grace Friscilla Margaretha Karo-Karo
I Gede Gilang Dharma Suputra
Dzakwan Al-Dzaky Bewasana
Erfandra Ramadhan Susanto
Siti Manyra Sabiya

PERISET

Indy Rahmadhona
Dhea Septi Kurnia Dati
Naufal Madega Pratama
M. Syihaab Al Faaruq
Shalihati Mutiara

PENERBIT

DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI BADAN SIBER DAN SANDI NEGARA

Jl. Harsono RM 70 Ragunan, Pasar Minggu, Jakarta Selatan,
12550

Telp. +62 21 780 5814

Fax. +62 21 7884 4104

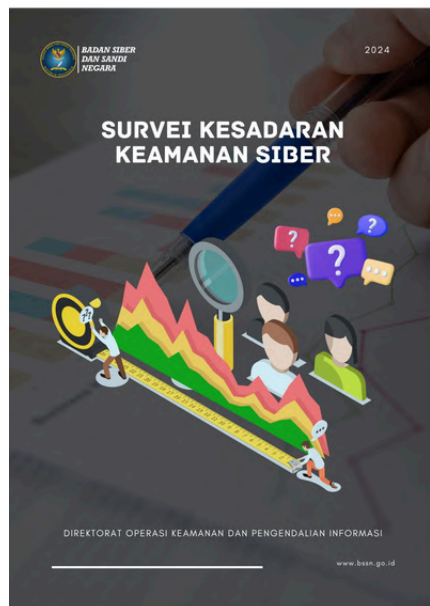
UKURAN :

E-ISBN :

ISBN :

CETAKAN PERTAMA : JANUARI 2025

Hak Penerbitan ©2024 Badan Siber dan Sandi Negara
Dilarang mengutip dan memperbanyak tanpa izin tertulis dari penerbit, sebagian atau seluruhnya dalam bentuk apa pun, baik cetak, *photoprint*, *microfilm*, dan sebagainya.



Kata Pengantar

“Privacy — like eating and breathing — is one of life’s basic requirements.” — Katherine Neville

Jumlah serangan siber terus meningkat dalam beberapa tahun terakhir. Bentuk ancaman siber juga semakin beragam sejalan dengan perkembangan teknologi informasi dan komunikasi. Faktor manusia merupakan faktor utama dalam sistem keamanan. Manusia merupakan celah keamanan tertinggi jika tidak memiliki kesadaran terhadap pentingnya keamanan siber. Oleh karena itu, memiliki kesadaran keamanan siber yang baik adalah kunci untuk melindungi diri dan data pribadi dari ancaman siber yang terus berkembang.

Kesadaran keamanan siber merupakan kewajiban bagi semua individu mulai dari staf hingga level eksekutif. Setiap individu harus mengetahui dan memahami berbagai jenis ancaman siber, mengadopsi kebiasaan dan prosedur yang aman dalam penggunaan teknologi dan internet serta mengetahui cara merespons jika terjadi insiden siber. Sinergi antara setiap individu dari berbagai level diperlukan agar kesadaran keamanan menjadi suatu kebiasaan (habit) dan dapat menciptakan budaya keamanan siber di organisasi bahkan negara.

Tolok ukur terwujudnya budaya keamanan siber di dalam masyarakat Indonesia dapat diketahui melalui alat ukur tingkat kesadaran keamanan siber. Tingkat kesadaran keamanan siber masyarakat Indonesia dapat terukur melalui suatu nilai indeks yang merepresentasikan sejauh mana kesadaran keamanan siber telah menjadi bagian dari perilaku dan kebiasaan sehari-hari masyarakat Indonesia. Untuk mengetahui tingkat kesadaran keamanan siber masyarakat Indonesia, BSSN melakukan pengkajian dan penyusunan instrumen alat ukur tingkat kesadaran keamanan siber masyarakat Indonesia yang akan menjadi instrumen Survei Kesadaran Keamanan Siber (SKKS).

BSSN terus berupaya dalam meningkatkan kesadaran keamanan siber masyarakat Indonesia melalui berbagai macam program budaya keamanan siber. Kesadaran keamanan siber bukan tanggung jawab BSSN semata, namun seluruh stakeholder terkait. Oleh karena itu, BSSN selalu mengajak dan melibatkan seluruh *stakeholder* terkait meliputi akademisi, pemerintah, praktisi dan masyarakat secara umum. BSSN menyadari bahwa kesadaran keamanan siber atau *cyber security awareness* merupakan investasi jangka panjang yang harus dilakukan oleh setiap individu dan berdampak bagi negara.

Dengan bangga kami persembahkan buku **“Survei Kesadaran Keamanan Siber”**. Buku ini merupakan buku pertama hasil prediksi tingkat kesadaran keamanan siber berdasarkan survei pada Generasi Z. Gen Z atau generasi dengan kelahiran di antara tahun 1997 sampai 2012 termasuk ke dalam pengguna internet terbanyak di Indonesia sehingga perlu dilakukan pengukuran tingkat kesadaran keamanan siber. Survei Kesadaran Keamanan Siber bertujuan untuk mengukur sejauh mana nilai kesadaran keamanan siber baik secara individu maupun secara nasional sebagai wujud kesiapan Gen Z sebagai pemuda calon pemimpin bangsa di masa Indonesia Emas 2045. Di masa mendatang, kami berharap pengukuran tingkat kesadaran keamanan siber dapat dilakukan di seluruh lapisan masyarakat tidak hanya pada Gen Z.



SATRYO SURYANTORO, S.Sos.

Direktur Direktorat Operasi Keamanan Dan
Pengendalian Informasi Badan Siber dan
Sandi Negara

Kami mengapresiasi seluruh stakeholder terkait serta Disdik dan Diskominfo di 34 provinsi yang telah mendukung proses kegiatan survei dari awal hingga akhir. Kami berharap kerja sama yang baik ini dapat diteruskan dan ditingkatkan agar memperoleh hasil yang semakin baik.

Akhir kata, semoga buku **“Survei Kesadaran Keamanan Siber”** ini dapat dimanfaatkan sebagai bentuk pertanggungjawaban bagi Badan Siber dan Sandi Negara secara khusus dan masyarakat secara umum. Selain itu, semoga buku ini dapat memberikan wawasan yang berharga bagi semua pihak untuk menjaga ruang siber Indonesia.

Daftar Isi

i	Kata Pengantar
iii	Daftar Isi
iv	Daftar Gambar
v	Daftar Grafik
1	Pendahuluan
16	Teori
25	Hasil dan Pembahasan
50	Penutup
62	Referensi
63	Lampiran

Daftar Gambar

Gambar 1.1	4
Gambar 1.2	5
Gambar 1.3	11
Gambar 1.4	11
Gambar 1.5	12
Gambar 1.6	12

Daftar Grafik

Grafik 1.1	8
Grafik 1.2	13
Grafik 3.1	22
Grafik 3.2	24
Grafik 3.3	28
Grafik 4.1	46
Grafik 4.2	46
Grafik 4.3	47
Grafik 4.4	47
Grafik 4.5	48
Grafik 4.6	48
Grafik 4.7	49
Grafik 4.8	49
Grafik 4.9	50
Grafik 4.10	50
Grafik 4.11	51

Daftar Tabel

Tabel 1.1	9
------------------------	----------

BSSN

2024

PENDAHULUAN



Isu Keamanan Siber di Kalangan Pelajar

Aktivitas online di kalangan pelajar ibarat menjelajah lautan luas. Selama berlayar, kita dapat memancing, menemui keindahan pulau-pulau, hewan laut dan pemandangan lainnya yang tidak kita jumpai ketika di darat. Akan tetapi, kita tidak dapat memprediksi akan adanya bahaya yang akan terjadi, seperti badai tak terduga, cuaca buruk, hiu yang lapar bahkan hewan laut buas lainnya yang mengintai di laut dalam. Tanpa peta, kapal canggih dan perlengkapan keamanan berlayar yang memadai, perjalanan yang penuh potensi ini bisa berubah menjadi petualangan berbahaya. Begitu pula dengan ruang siber— **keamanan siber bagaikan gunung es**. Risiko ancaman siber yang tampak hanya di puncak gunung es. Namun, setidaknya ada 7/8 gunung es yang terendam air. Di sinilah kita dapat menemukan banyak **risiko ancaman siber** yang mengintai. Oleh karena itu, kita perlu waspada dan memperoleh wawasan yang lebih mendalam tentang semua risiko keamanan siber.

Perkembangan teknologi, khususnya **internet** dan **media sosial**, memudahkan pelajar SMA mengakses informasi dengan cepat, namun seringkali **belum** dilengkapi dengan **pengetahuan yang memadai** tentang perlindungan diri secara digital. Tantangan keamanan siber ini muncul karena **rendahnya tingkat kesadaran** para pelajar terhadap dasar-dasar praktik keamanan siber, baik keamanan siber secara teknis maupun keamanan siber sosial. Melihat situasi ini, diperlukan pemetaan kesadaran keamanan siber pelajar yang dapat memberikan gambaran mengenai kondisi tingkat kesadaran keamanan siber pelajar Indonesia.



Dengan demikian, **pelaksanaan survei kesadaran keamanan siber** ini menjadi **langkah awal** dalam pelaksanaan **penguatan pengetahuan keamanan siber** yang memadai dan lebih lanjut dapat mengetahui tingkat kesadaran keamanan siber pelajar Indonesia melalui indeks nasional.

**ISU KEAMANAN
SIBER**

**DI KALANGAN
PELAJAR**

Berdasarkan hasil survei akademis dari Universitas Indonesia (2023), hanya **sekitar 40%** pelajar SMA yang **memahami risiko siber** yang dapat mengancam mereka di media sosial. Sayangnya, meskipun mereka menyadari ancaman tersebut, sebagian besar masih **enggan** untuk **menerapkan langkah-langkah keamanan dasar** pada akun pribadi mereka. Minimnya kesadaran tentang keamanan siber di kalangan pelajar menyebabkan mereka rentan terhadap serangan, sehingga penting untuk mengukur dan meningkatkan pemahaman mereka terkait ancaman siber yang bisa saja mengancam keamanan dan privasi mereka secara langsung.



Pentingnya survei kesadaran keamanan siber ini sejalan dengan **Peraturan BSSN Nomor 5 Tahun 2022**, yang menekankan perlunya penguatan edukasi di sektor publik. Survei yang dilakukan pada **34 provinsi** di Indonesia ini diharapkan bisa memberikan gambaran yang lebih jelas tentang tingkat kesadaran individu terhadap ancaman siber, serta menjadi langkah awal dalam merumuskan strategi peningkatan budaya keamanan siber. **Keamanan Siber Teknis** dan **Sosial** merupakan 2 variabel besar dalam **ruang lingkup** survei ini.

Metodologi

Metodologi pelaksanaan kegiatan Survei Kesadaran Keamanan Siber meliputi Persiapan: Persiapan Administrasi dan Survei; Pengumpulan Data: penetapan responden dan lokasi, penentuan target responden, pengambilan data; Pengolahan Data dan Analisis Data; dan Penyusunan Laporan. Berikut penjelasan pada setiap tahap metodologi survei tersebut, yaitu:



Gambar 1.1 Bagan Metodologi Survei Kesadaran Keamanan Siber

Persiapan Administratif

Tahap persiapan administratif dititik beratkan pada proses koordinasi dengan stakeholder terkait, yang terdiri dari:

- 1 Rapat Pembahasan Teknis Survei dengan Dinas Pendidikan dan Dinas Komunikasi dan Informatika seluruh Provinsi via Zoom.
- 2 Dinas Pendidikan seluruh Provinsi mengirim surat penunjukan ke sekolah yang menjadi target responden survei.
- 3 Perwakilan tiap sekolah seluruh Provinsi mengisi link narahubung untuk dapat dikirimkan link survei.
- 4 Perwakilan tiap sekolah seluruh Provinsi mengarahkan survei kepada para pelajar di sekolah tersebut.



Gambar 1.2 Alur Pengambilan Data



Penentuan Variabel

Variabel penilaian Survei Kesadaran Keamanan Siber terdiri dari variabel Keamanan Siber Teknis dan variabel Keamanan Siber Sosial. Kemudian dari dua variabel tersebut, diturunkan menjadi beberapa indikator. Indikator masing-masing variabel yang digunakan adalah sebagai berikut:

KEAMANAN SIBER TEKNIS

- 1 Syarat dan Ketentuan Instalasi Perangkat / Aplikasi
- 2 Kata Sandi (Password)
- 3 Internet dan Wifi
- 4 Keamanan Perangkat
- 5 Aduan Insiden Siber Teknis
- 6 Hukum dan Regulasi Keamanan Siber Teknis

KEAMANAN SIBER SOSIAL

- 7 Rekayasa Sosial (Social Engineering)
- 8 Konten Negatif
- 9 Aktivitas Media Sosial
- 10 Aduan Insiden Siber Sosial
- 11 Hukum dan Regulasi Keamanan Siber Sosial

Penyusunan Kuesioner

Penyusunan kuesioner Survei Kesadaran Keamanan Siber dibagi menjadi 3 (tiga) bagian sesuai dengan tujuan survei, yaitu :

BAGIAN I

Identitas responden, meliputi: wilayah survei, nama, nomor telepon/HP, usia, jenis kelamin, asal sekolah, nama sekolah.

Saran, opini atau pendapat bebas dari responden

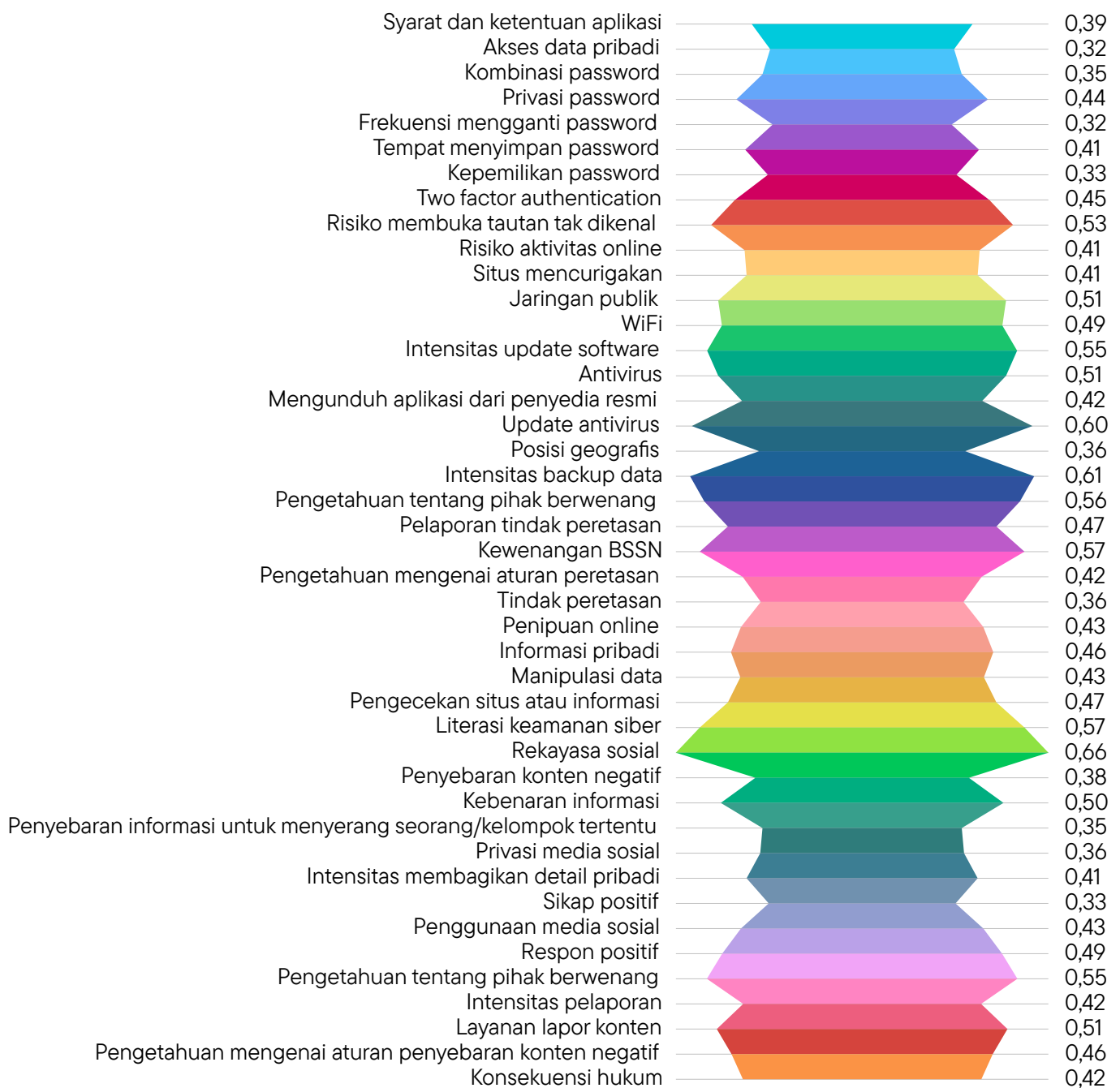
BAGIAN II

- Syarat dan Ketentuan Instalasi Perangkat/Aplikasi
- Kata Sandi (Password)
- Internet dan Wifi
- Keamanan Perangkat
- Aduan Insiden Siber Teknis
- Hukum dan Regulasi Keamanan Siber Teknis
- Rekayasa Sosial (Social Engineering)
- Konten Negatif
- Aktivitas Media Sosial
- Aduan Insiden Siber Sosial
- Hukum dan Regulasi Keamanan Siber Sosial

Uji Validitas dan Reliabilitas

a. Hasil Uji Validitas

Uji Validitas bertujuan untuk **menguji ketepatan alat ukur** dan memastikan **kualitas data** bagi pengambil keputusan. Setelah dikumpulkan, data diuji validitasnya menggunakan **SPSS (Cronbach's Alpha)** sebelum diolah dan dipublikasikan. Hasil uji validitas variabel dan indikator survei kesadaran keamanan siber adalah sebagai berikut:



Grafik 1.1 Hasil Uji Validitas

Validitas item pertanyaan ditunjukkan dengan adanya **korelasi skor item** pertanyaan terhadap **skor total seluruh item pertanyaan**. Perhitungan dilakukan dengan cara mengkorelasikan antara skor item dengan skor total seluruh item pertanyaan. Pertanyaan dikatakan **valid** apabila nilai korelasi lebih besar dari **r tabel** untuk **$\alpha = 5\%$ yaitu 0,203**.



Pada survei kesadaran keamanan siber telah ditetapkan bahwa terdapat **43 atribut** yang nantinya akan ditanyakan. Kuesioner tersebut telah disebar pada **3 provinsi (Sulawesi Tenggara, Kalimantan Timur, Daerah Istimewa Yogyakarta)** yang dipilih secara acak. Dari 43 atribut tersebut, **semuanya dinyatakan valid** dikarenakan semua atribut untuk **nilai korelasinya $> r$ tabel**. Hasil dari 43 atribut tersebut dinyatakan **valid dengan nilai $\alpha > 0,203$** .



b. Hasil Uji Reabilitas

Untuk **uji reliabilitas** diukur pada **nilai Cronbach's Alpha** yang didapatkan dari **hasil uji reliabilitas**, jika nilai Cronbach's Alpha **lebih besar dari 0,6** maka jawaban dari para responden pada kuesioner sebagai alat pengukur dinilai **reliabel**. Jika Cronbach's Alpha **lebih kecil dari 0,6** maka jawaban para responden dinyatakan **tidak reliabel**.

Dari **hasil uji reliabilitas** di atas dapat dilihat **kuesioner** survei kesadaran keamanan siber adalah **reliabel**, dikarenakan pada kuesioner survei kesadaran keamanan siber **nilai $\alpha = 0.906 > 0.6$** .



Cronbach's Alpha	N of Items
.906	43

Tabel 1.1 Hasil Uji Reliabilitas

Pengumpulan Data

Tahapan pengumpulan data terdiri dari tiga jenis tahapan yaitu penetapan responden dan lokasi, penentuan target responden, dan pengambilan data. Teknik pengumpulan data Survei Kesadaran Keamanan Siber dilakukan dengan menggunakan kuesioner elektronik.

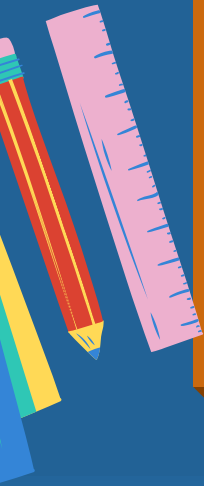


Penetapan Responden dan Lokasi

Responden pada kegiatan Survei Kesadaran Keamanan Siber adalah **generasi Z** yang diwakilkan oleh siswa-siswi **Sekolah Menengah Atas (SMA)** atau sederajat. Alasan pemilihan siswa-siswi SMA atau sederajat dipilih menjadi responden survei yaitu sebagai berikut:



1. Siswa SMA lebih familiar dalam penggunaan internet dibandingkan dengan siswa SMP (APJII, 2022).
2. Berada dalam rentang usia aktif menggunakan internet.
3. Menggunakan internet untuk berbagai kegiatan.
4. Masa transisi dari anak-anak menuju dewasa.



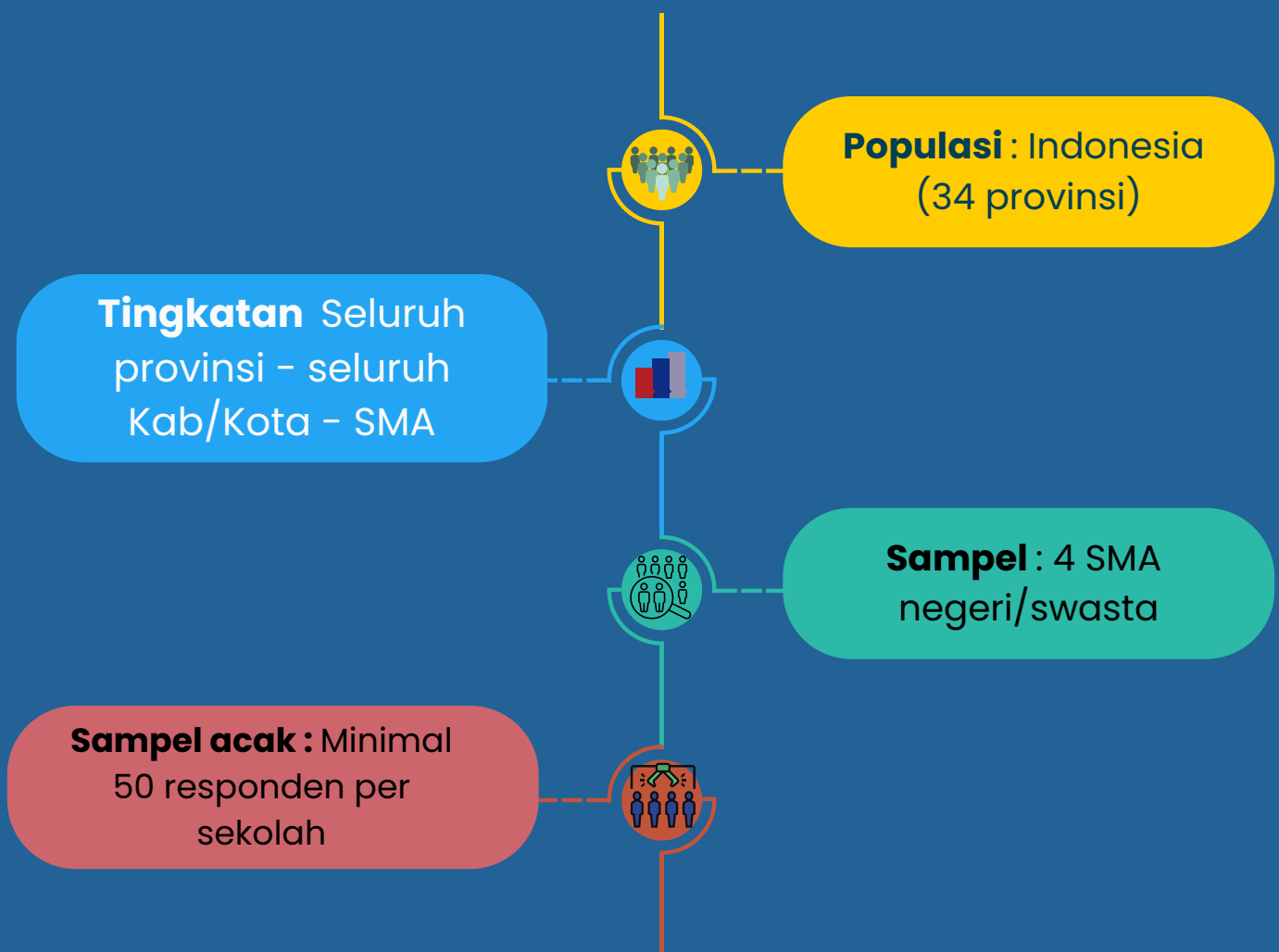
Penentuan Target Responden

Penentuan target responden dilakukan menggunakan **rumus slovin** pada Survei Kesadaran Keamanan Siber. Penentuan target responden untuk menentukan **sampel minimum** menggunakan rumus sebagai berikut:

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

n : ukuran sampel
N : ukuran populasi
e : tingkat signifikansi

Gambar 1.3 Perhitungan Jumlah Sampel Minimum dengan Rumus Slovin



Gambar 1.4 Penentuan Responden

3. Pengolahan Data dan Analisis Data

Nilai kesadaran keamanan siber teknis dan nilai kesadaran keamanan siber sosial merupakan nilai rata-rata dari indikator dari tiap besaran isu (variabel). Perhitungan nilai kesadaran keamanan siber teknis dan nilai kesadaran keamanan siber sosial dijabarkan sebagai berikut.

$$NK_{KST} = \frac{\sum_{i=1}^j I_{KST}}{j} \qquad NK_{KSS} = \frac{\sum_{i=1}^k I_{KSS}}{k}$$

j : Jumlah indikator pada variabel Keamanan Siber Teknis

I_{KST} : Nilai indikator pada variabel Keamanan Siber Teknis

k : Jumlah indikator pada variabel Keamanan Siber Sosial

I_{KSS} : Nilai indikator pada variabel Keamanan Siber Sosial

Gambar 1.5 Perhitungan nilai kesadaran keamanan siber teknis dan nilai kesadaran keamanan siber sosial

Nilai indikator pada tiap besaran isu (variabel) diperoleh dari jumlah nilai skor jawaban dibagi dengan nilai maksimal skor jawaban. Perhitungan nilai indikator tiap variabel dijabarkan sebagai berikut.

$$I_x = \frac{\text{jumlah nilai skor pernyataan}}{\text{nilai maks pernyataan}} \times 100$$

I_x : Nilai indikator di variabel survei

X : Indikator pada variabel Keamanan Siber Teknis atau variabel Keamanan Siber Sosial

Gambar 1.6 Perhitungan nilai indikator tiap variabel

3.2 Analisa Data

Data yang telah masuk, akan dianalisa secara manual maupun dengan menggunakan aplikasi Surveiku.com, dan software statistik SPSS. Pengolahan data akan menghasilkan output Nilai Indeks Kesadaran Keamanan Siber (IKKS).



Grafik 1.2 Nilai Indeks Kesadaran Keamanan Siber (IKKS)

- Memiliki tingkat kesadaran keamanan siber yang sangat rendah (**Buruk**)
- Memiliki tingkat kesadaran keamanan siber yang rendah (**Kurang Baik**)
- Memiliki tingkat kesadaran keamanan siber yang tinggi (**Baik**)
- Memiliki tingkat kesadaran keamanan siber yang sangat tinggi (**Sangat Baik**)

Tahapan akhir berisi kesimpulan terhadap hasil Indeks Kesadaran Keamanan Siber (IKKS), serta saran rekomendasi tindak lanjut yang harus dilakukan terutama pada sub indikator (area) yang mempunyai nilai kurang baik.

4. Penyusunan Laporan

Hasil pelaksanaan seluruh kegiatan Survei Kesadaran Keamanan Siber yang telah dilakukan akan disusun dalam Laporan Akhir untuk diserahkan kepada pihak terkait.



BSSN

2024

DEFINISI OPERASIONAL VARIABEL



KEAMANAN SIBER TEKNIS



KEAMANAN SIBER SOSIAL

Keamanan siber teknis mengacu pada serangkaian langkah dan teknologi yang dirancang untuk **melindungi sistem, jaringan, dan data** dari serangan siber. Teknik keamanan yang dilakukan mencakup penerapan **firewall, antivirus, enkripsi data**, serta **pengelolaan akses pengguna**. Selain itu, keamanan teknis juga mencakup **pelindungan data sensitif** seperti **informasi pribadi** dan **finansial**.

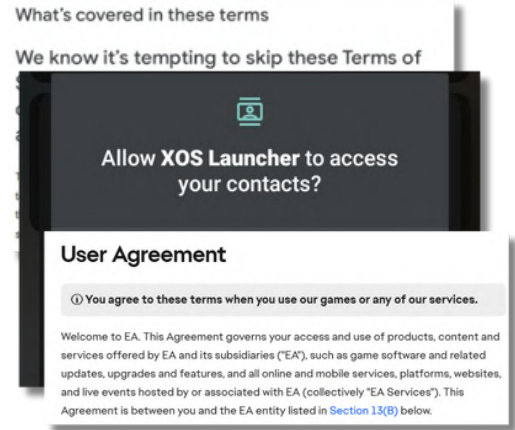


Keamanan siber sosial mencakup upaya **melindungi manusia** baik **individu** maupun **kelompok** dari **praktik-praktik manipulasi sosial** di **ruang siber**. Teknik serangan siber sosial yang digunakan antara lain **phising, rekayasa sosial**, dan **penyebaran konten yang bertentangan peraturan perundang-undangan seperti hoaks dan cyberbullying**. Serangan siber sosial memanfaatkan **kelemahan atau celah** dari sisi **manusia** untuk memperoleh **informasi sensitif** dengan tujuan **mengakses sistem tertentu bahkan mempengaruhi opini publik di ruang siber**.

Keamanan Siber Teknis

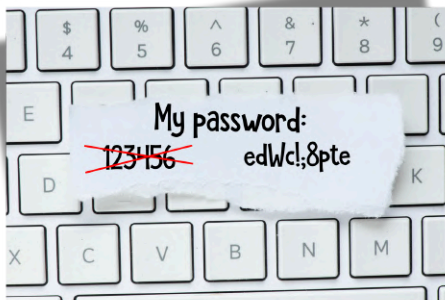
Syarat dan Ketentuan Instalasi Perangkat/Aplikasi

Indikator ini mencakup kesadaran dan perilaku individu saat menginstal suatu aplikasi. Individu harus **memahami** syarat dan ketentuan yang ditawarkan aplikasi. Hal ini berarti bahwa individu juga telah paham akan **risiko** saat menginstal aplikasi. Aplikasi terbuka (*open source*) tidak serta merta gratis karena aplikasi tersebut bisa saja mengakses data pribadi tanpa izin, memanfaatkan perangkat untuk aktivitas berbahaya, atau menjadi celah disusupi malware.



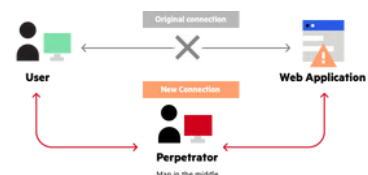
Kata Sandi (Password)

Indikator ini mencakup kesadaran dan perilaku individu saat **membuat** dan **menggunakan kata sandi (password)**. Penggunaan kata sandi yang lemah, mudah ditebak, atau sama untuk banyak akun dapat meningkatkan **risiko pencurian data** dan **akses tidak sah** ke sistem.



Internet dan Wifi

Indikator ini mencakup kesadaran dan perilaku individu saat membuka tautan yang **tak dikenal**, menggunakan jaringan WiFi publik. Jaringan WiFi publik **tanpa enkripsi**, dapat memungkinkan **serangan** seperti man-in-the-middle (MITM), pencurian data, atau penyadapan komunikasi.



Keamanan Siber Teknis

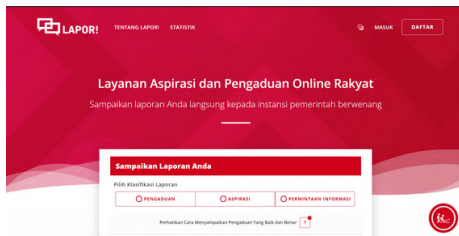


Keamanan Perangkat

Indikator ini mencakup kesadaran dan perilaku individu untuk melindungi perangkat digital dari berbagai serangan siber teknis. Upaya pencegahan serangan siber teknis yang dilakukan berupa pemasangan **antivirus**, **menonaktifkan posisi geografis perangkat digital** saat tidak digunakan dan **backup data** pada perangkat untuk keamanan data.

Aduan Insiden Siber Teknis

Indikator ini mencakup kesadaran dan perilaku individu saat mengalami, menemukan atau mengajukan laporan insiden siber teknis kepada pihak berwenang atau lembaga seperti BSSN melalui kanal layanan aduan. Hal ini juga merupakan pengetahuan individu terhadap mekanisme pelaporan dan kewenangan BSSN dalam menangani Insiden siber teknis. Insiden siber teknis yang dapat dilaporkan antara lain web phishing, web defacement, peretasan akun digital, forensik digital dan insiden siber teknis lainnya. Aduan insiden siber teknis bertujuan untuk mengurangi dampak, memperbaiki sistem terdampak, maupun mencegah insiden yang sama terjadi.



Keamanan Siber Teknis

Hukum dan Regulasi Keamanan Siber Teknis

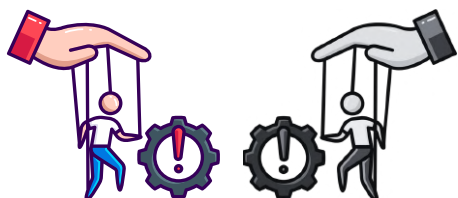
Indikator ini mencakup kesadaran dan perilaku individu dalam mengetahui, memahami dan menerapkan hukum dan regulasi yang mengatur keamanan siber teknis. Indikator ini bertujuan untuk menilai kepatuhan individu terhadap peraturan perundangan yang mengatur keamanan siber teknis.



Keamanan Siber Sosial

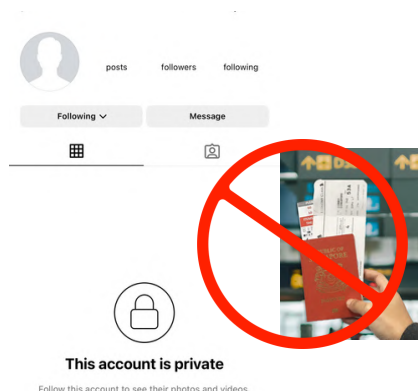
Rekayasa Sosial

Indikator ini mencakup kesadaran dan perilaku individu terhadap mencegah praktik rekayasa sosial. Praktik rekayasa sosial merupakan metode manipulasi psikologis oleh pelaku kejahatan siber untuk membujuk atau menipu individu agar memberikan informasi sensitif, seperti kata sandi, data pribadi, atau akses ke sistem tertentu.



Konten Negatif

Indikator ini mencakup kesadaran dan perilaku individu saat membuat dan menyebarkan konten digital. Konten digital tersebut apakah memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan, atau penyebaran berita bohong yang berpotensi merugikan pihak tertentu secara materiil atau non-materiil.



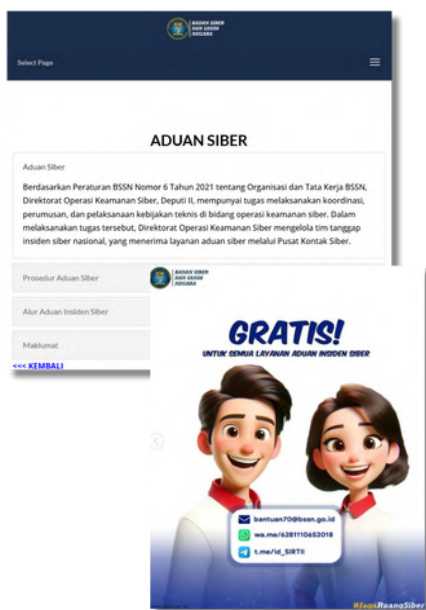
Aktivitas Media Sosial

Indikator ini mencakup kesadaran dan perilaku individu saat menggunakan platform media sosial. Penilaian keamanan siber saat mengakses platform media sosial terdiri dari semua tindakan seperti pengaturan privasi, membagikan informasi pribadi, sikap positif saat membagikan konten serta dampak penggunaan media sosial berlebihan bagi produktivitas dan kesehatan mental.

Keamanan Siber Sosial

Aduan Insiden Siber Sosial

Indikator ini mencakup kesadaran dan perilaku individu saat mengalami, menemukan atau mengajukan laporan insiden siber sosial kepada pihak berwenang atau lembaga seperti BSSN melalui kanal layanan aduan. Hal ini juga merupakan pengetahuan individu terhadap mekanisme pelaporan dan kewenangan BSSN dalam menangani Insiden siber sosial. Insiden siber sosial yang dapat dilaporkan antara lain konten negatif berdasarkan UU ITE dan insiden siber sosial lainnya. Aduan insiden siber sosial bertujuan untuk mengurangi dan memperbaiki dampak, serta mencegah insiden yang sama terjadi.



Hukum dan Regulasi Keamanan Siber Sosial

Indikator ini mencakup kesadaran dan perilaku individu dalam mengetahui, memahami dan menerapkan hukum dan regulasi yang mengatur keamanan siber sosial. Indikator ini bertujuan untuk menilai kepatuhan individu terhadap peraturan perundangan yang mengatur keamanan siber sosial.

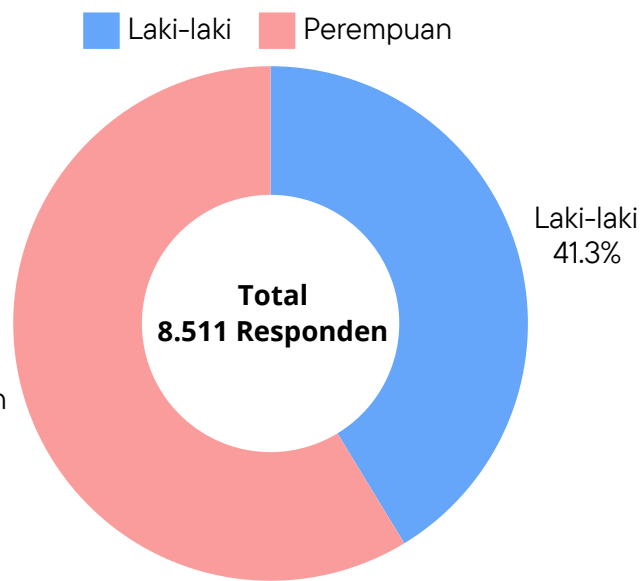




Indeks Kesadaran Keamanan Siber Nasional

Profil Responden

Responden merupakan pelajar dengan rentang usia 14-18 tahun dengan total responden sebanyak 8511 responden. Dari total **8511 responden**, pembagian populasi berdasarkan jenis kelamin adalah sebanyak **3518 responden laki-laki** dan **4993 responden perempuan** sesuai dengan grafik berikut:



Perempuan
58.7%

Laki-laki
41.3%

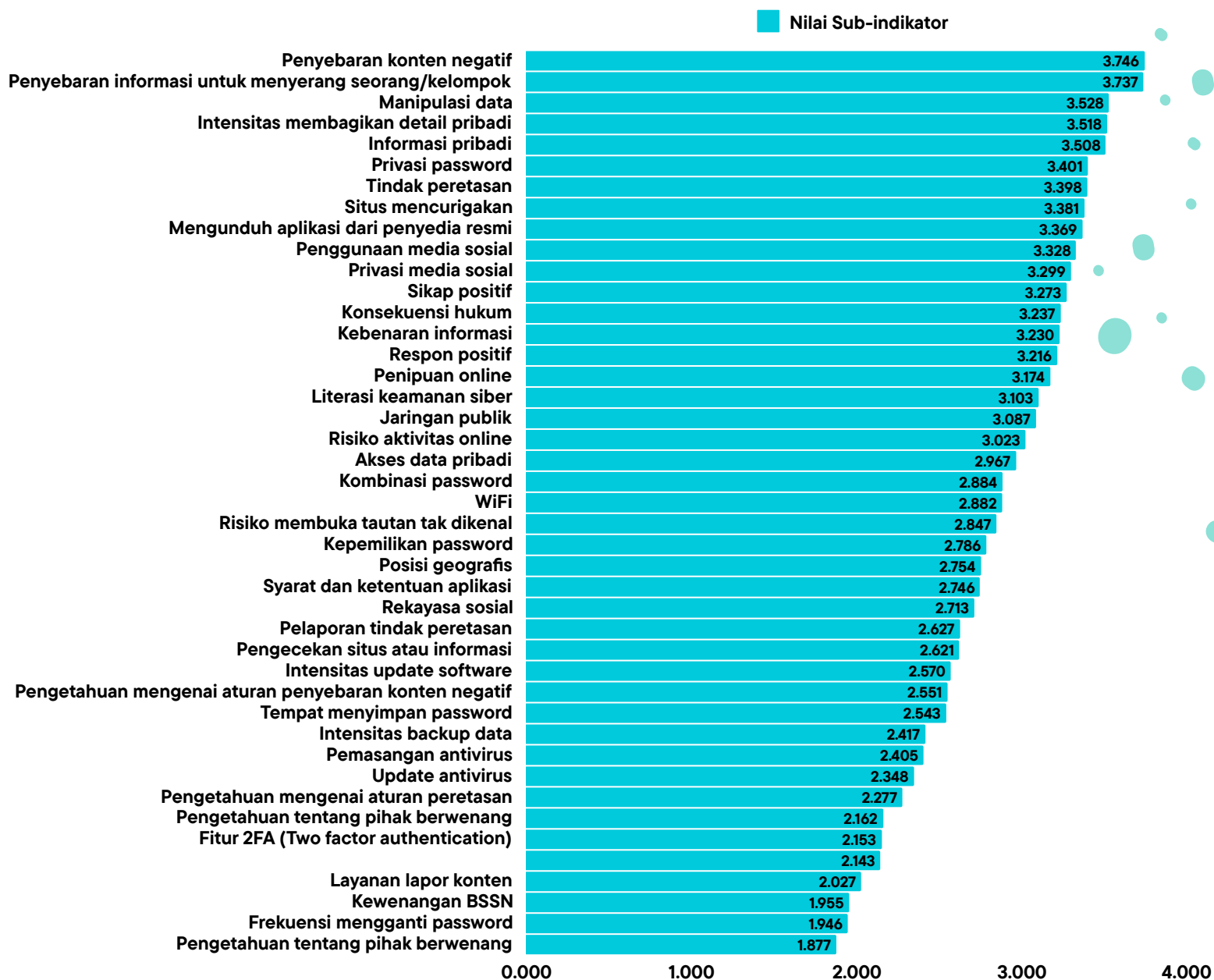
Grafik 3.1 Persentase Jenis Kelamin Responden



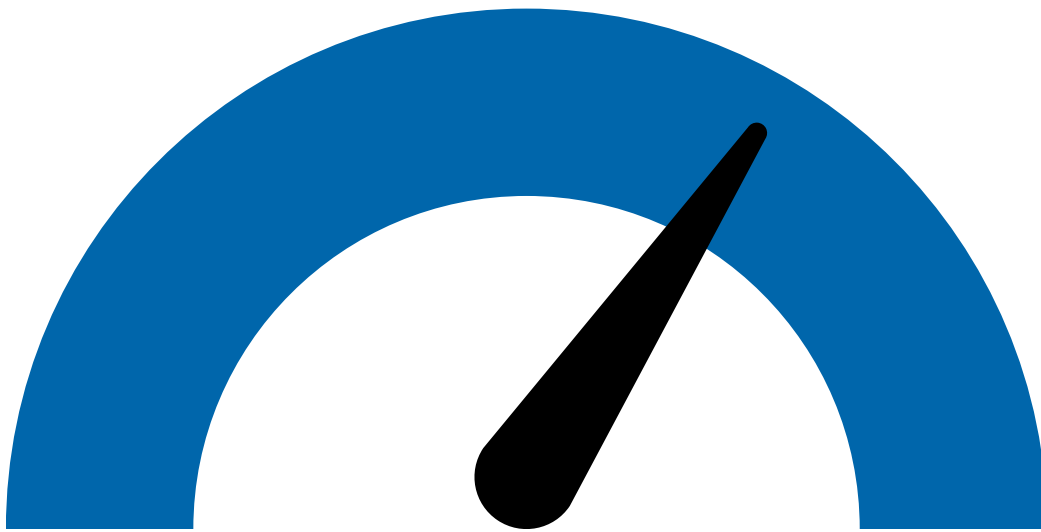
Tingkat Kesadaran Keamanan Siber

Indeks Kesadaran Keamanan Siber Tahun 2024 pada tingkat pelajar SMA sederajat yaitu **2,855** dengan **kategori Baik**.

Tiap sub-indikator pada survei kesadaran keamanan siber juga dilakukan pengukuran dengan rincian indeks tiap sub-indikator dapat dilihat pada gambar di bawah. Terdapat 3 sub-indikator dari 43 sub-indikator yang mendapatkan kategori kurang baik, yaitu unsur **frekuensi mengganti password, pengetahuan tentang pihak berwenang, dan kewenangan BSSN**.



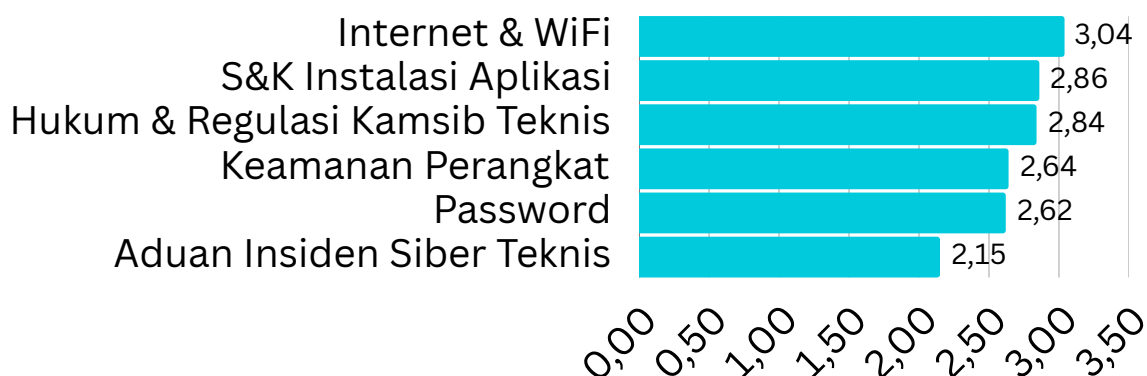
Variabel Keamanan Siber Teknis



2,69 dari 4,00

Indeks Variabel Keamanan Siber Teknis

Variabel **keamanan siber teknis** memiliki indeks sebesar **2,69**. Indeks tersebut berarti bahwa kesadaran keamanan siber teknis tingkat pelajar SMA sederajat sudah **TINGGI** dengan kategori **BAIK**. Indikator yang menjadi perhatian **khusus** yaitu Aduan Insiden Siber Teknis dengan indeks paling rendah yaitu sebesar **2,15**.



Grafik 3.2 Indeks Tiap Sub-Indikator dari Variabel Keamanan Siber Teknis

Breaking News

Keamanan Siber Teknis

Internet dan WiFi

Hampir setiap orang menggunakan jaringan WiFi publik saat di kafe, bandara dan tempat umum lainnya untuk tetap terkoneksi dengan dunia maya termasuk pelajar SMA sederajat. Mereka terbiasa belajar, bermain game online, bahkan melakukan transaksi perbankan dengan menggunakan jaringan WiFi publik. Mereka masih banyak menggunakan WiFi publik hanya untuk mendapatkan jaringan data internet secara gratis. Namun begitu, penggunaan WiFi di tempat umum tetap harus waspada karena ada celah keamanan siber yang memungkinkan peretas membuat jaringan WiFi palsu atau menyusupi jaringan yang sudah ada.

Celah keamanan ini ditemukan dalam desain standar protokol WiFi IEEE 802.11, yang memungkinkan peretas mengelabui titik akses untuk membocorkan frame jaringan WiFi dalam bentuk plaintext. Frame WiFi merupakan wadah data yang terdiri dari header, muatan data, dan trailer, yang mencakup informasi seperti alamat MAC sumber dan tujuan, kontrol, dan data manajemen.

Jika pengguna WiFi publik sudah terperangkap dalam jaringan WiFi palsu tersebut, peretas dapat dengan leluasa mengambil informasi pribadi seperti login media sosial, detail perbankan, dan alamat email yang rentan penyalahgunaan. Bahkan, dengan modal tersebut peretas dapat mengurus rekening korbannya.

Jika terpaksa terkoneksi dengan WiFi publik, khususnya ketika melakukan transaksi penting, pengguna lebih baik menggunakan Virtual Private Network (VPN).

S&K Instalasi Perangkat/Aplikasi

Syarat dan ketentuan (S&K) pada suatu aplikasi adalah perjanjian hukum antara penyedia perangkat atau aplikasi dengan pengguna aplikasi. Oleh karena itu membaca dan memahami syarat dan ketentuan perangkat atau aplikasi sangat penting.

S&K biasanya berisi tentang: hal dan kewajiban pemilik dan pengguna aplikasi; batasan tanggung jawab pemilik dan pengguna aplikasi; pengaturan pembayaran; penyelesaian sengketa; kebijakan privasi yang berkaitan dengan perlindungan data pribadi saat menggunakan aplikasi.

Jika asal klik setuju, artinya pengguna memperbolehkan aplikasi untuk mengelola data untuk kepentingan lain. Bahkan untuk tindakan yang mengganggu, seperti: menjual data pribadi kepada pihak lain; mendapat pesan atau telepon dari orang tak dikenal.

Oleh karena itu, hal yang perlu pengguna cermati saat membaca S&K sebelum menginstal aplikasi yaitu memahami bagian kebijakan privasi; artinya pengguna dapat mengetahui perlindungan yang akan diberikan oleh penyedia aplikasi terhadap data pribadi.

Selain itu, jika terjadi kebocoran data pribadi dari satu akun sistem elektronik, maka pengguna harus merubah kata sandi di perangkat elektronik lainnya jika memiliki kata sandi yang serupa. Pengguna juga dapat mengumpulkan bukti untuk dilaporkan kepada pihak berwajib. Perlindungan data pribadi dalam sistem elektronik diatur dalam Peraturan Menteri Kominfo No.20 Tahun 2016.

Keamanan Siber Teknis

Hukum dan Regulasi Keamanan Siber Teknis

Keamanan siber diatur dalam Perpres Nomor 47 tahun 2023 tentang strategi keamanan siber nasional dan manajemen krisis siber. Berdasarkan perpres tersebut berarti pemerintah melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial.

Pengguna sebagai warga negara Indonesia harus memiliki pengetahuan dan kepatuhan terhadap hukum dan regulasi yang mengatur keamanan siber teknis. Pengaturan keamanan siber teknis mengacu pada Undang-Undang Informasi Transaksi Elektronik, antara lain pelanggaran yang dilakukan terhadap pasal 30, pasal 31, pasal 32, pasal 33, pasal 34, pasal 35, pasal 36 dan pasal 37.

Pengguna perlu menumbuhkan kesadaran terhadap peraturan yang berlaku. Pelanggaran terhadap hukum dan regulasi keamanan siber teknis mendapat sanksi sesuai dengan hukum dan regulasi keamanan siber teknis tersebut.

Keamanan Perangkat

Keamanan perangkat adalah praktik dan prosedur yang dilakukan untuk melindungi perangkat dari ancaman dan serangan yang merusak, seperti virus, malware, hacker, dan peretasan data. Tujuan utama dari keamanan perangkat adalah untuk melindungi data sensitif dan informasi rahasia dari kebocoran atau akses yang tidak sah. Keamanan perangkat mencakup sejumlah langkah dan teknologi untuk mencegah, mengidentifikasi, dan merespon ancaman siber teknis.

Upaya dan langkah keamanan siber teknis meliputi keamanan fisik meliputi pencegahan akses fisik yang tidak sah ke perangkat jaringan, seperti mengunci ruang server atau memasang sensor gerak dan kamera pengawas. Selain itu keamanan non-fisik meliputi pemasangan firewall, enkripsi data dan jaringan, deteksi dan karantina malware, menerapkan pembatasan akses seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan pemeriksaan identitas pengguna untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke jaringan serta manajemen patch untuk memperbarui perangkat lunak dan sistem operasi untuk memperbaiki kerentanan keamanan dan memastikan bahwa perangkat jaringan selalu diperbarui dengan versi yang terbaru.

Survei Kesadaran Keamanan Siber (SKKS) lebih fokus kepada perilaku individu sehari-hari. Oleh karena itu keamanan perangkat yang dimaksud lebih menitikberatkan pada perilaku individu saat menggunakan kata sandi yang kuat, autentikasi dua faktor serta rutin memperbarui sistem operasi aplikasi dan perangkat lunak.

Breaking News

Keamanan Siber Teknis

Kata Sandi (Password)

Pengguna membutuhkan kata sandi (password) pada mayoritas aktivitas online seperti memeriksa email atau perbankan online. Memang lebih mudah bagi pengguna untuk membuat dan mengingat password yang sederhana, tetapi ini berisiko pada keamanan siber. Pengguna sebaiknya membuat password yang tidak sulit diingat sendiri, namun sulit ditebak orang lain.

Mengapa pengguna membutuhkan password yang kuat? Faktanya adalah meskipun mayoritas website sudah aman, namun selalu ada kemungkinan orang lain berniat jahat mencoba untuk mengakses atau mencuri informasi pribadi (peretasan). Password yang kuat adalah salah satu cara untuk mempertahankan akun dan informasi pribadi dari upaya peretasan.

Pada umumnya, password yang dibuat mengandung unsur nama keluarga, hobi, atau pola sederhana lainnya. Password ini memang mudah diingat, tetapi kurang aman. Pengguna dapat membuat kombinasi password yang unik untuk setiap akun online.

Selain itu, pengguna dapat menggunakan aplikasi password manager untuk menyimpan password dengan aman daripada menuliskannya di kertas yang rentan hilang atau dicuri. Aplikasi password manager dapat mengingat dan berisi semua password pada website yang berbeda-beda, sehingga tidak perlu mengingatnya lagi.

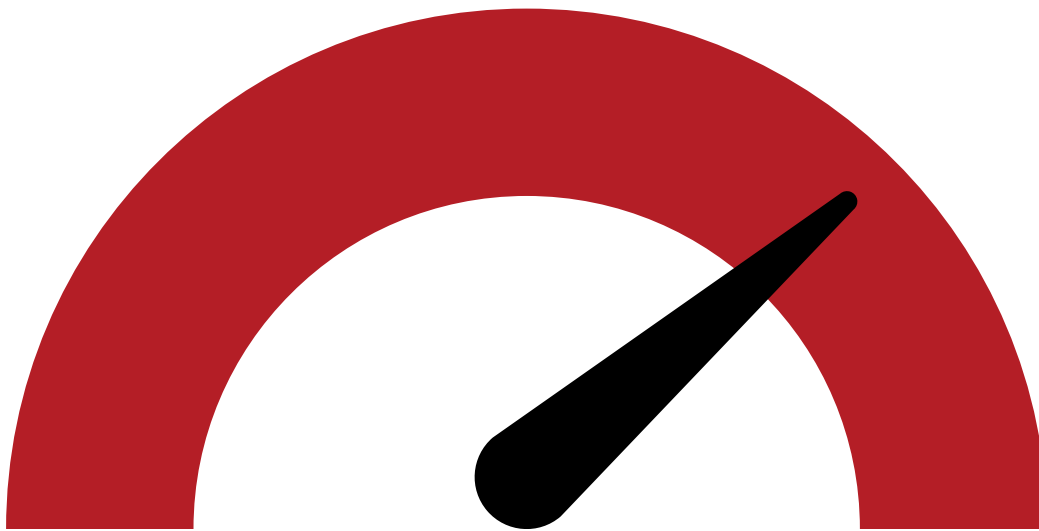
Aduan Insiden Siber Teknis

Beberapa instansi pemerintah termasuk BSSN melaksanakan upaya adaptif dan inovatif dengan memberikan layanan aduan insiden siber teknis. Insiden siber teknis yang dapat dilaporkan antara lain web phishing, web defacement, peretasan akun digital, forensik digital dan insiden siber teknis lainnya.

Pengguna dapat melaporkan insiden siber teknis kepada BSSN melalui alamat email: bantuan70@bssn.go.id atau nomor telepon 021 78833610. Pelapor diwajibkan mengikuti prosedur layanan aduan insiden siber teknis yang telah ditetapkan BSSN.

Selain BSSN, instansi pemerintah terkait seperti Komdigi dan Polri juga memiliki layanan aduan insiden siber teknis. Pelapor dapat memilih layanan aduan insiden siber teknis sesuai dengan kebutuhan tindak lanjut. Pelapor yang mengalami kerugian materiil dan membutuhkan penindakan dapat melapor kepada Ditipidsiber Polri. Pelapor insiden siber teknis juga harus mengikuti mekanisme pelaporan sesuai SOP layanan aduan yang diterapkan instansi pemerintah terkait.

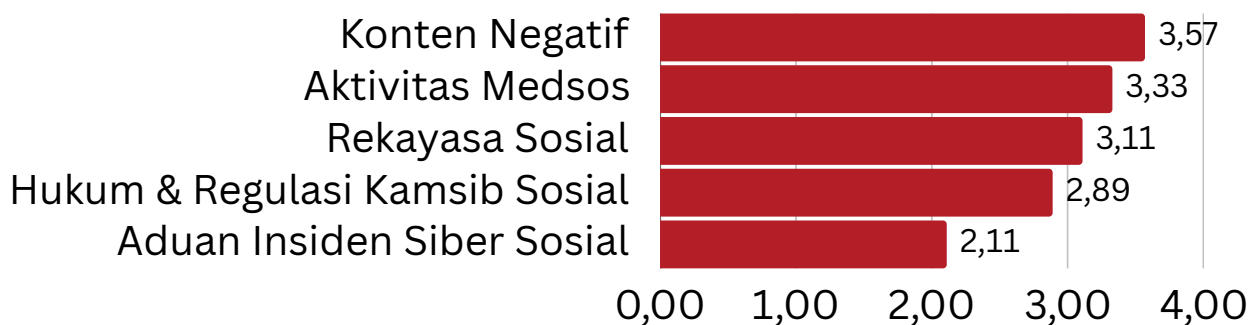
Variabel Keamanan Siber Sosial



3,00 dari 4,00

Indeks Variabel Keamanan Siber Sosial

Variabel **keamanan siber sosial** memiliki indeks sebesar **3,00**. Indeks tersebut berarti bahwa kesadaran keamanan siber teknis tingkat pelajar SMA sederajat sudah **SANGAT TINGGI** dengan kategori **SANGAT BAIK**. Indikator yang menjadi perhatian **khusus** yaitu Aduan Insiden Siber Sosial dengan indeks paling rendah yaitu sebesar **2,11**.



Grafik 3.3 Indeks Tiap Sub-Indikator dari Variabel Keamanan Siber Sosial

Breaking News

Keamanan Siber Sosial

Konten Negatif

Konten negatif mencakup tindakan yang dikategorikan sebagai perbuatan dilarang oleh negara berdasarkan UU ITE. Konten negatif yang dimaksud antara lain informasi bermuatan pornografi, pelecehan dan eksploitasi seksual, pencemaran nama baik, pemerasan, berita bohong/hoaks, Suku, Agama, Ras dan Antargolongan (SARA) dan Cyberbullying.

Pemerintah Indonesia termasuk BSSN terus memperkuat langkah-langkah pemberantasan penyebaran konten negatif yang dianggap merusak tatanan sosial, ekonomi, dan moral masyarakat. Dalam upaya ini, berbagai strategi diterapkan, termasuk penguatan literasi keamanan siber dan pemblokiran situs, konten dan akun penyebar konten negatif. Pendekatan komprehensif ini melibatkan sejumlah kementerian, lembaga, dan pemangku kepentingan lainnya yang bekerja sama untuk menciptakan ruang siber yang aman dan sehat.

Aktivitas Media Sosial

Menggunakan media sosial sudah tidak Media sosial merupakan media untuk berkomunikasi, selalu terkoneksi dan berbagi cerita dengan orang lain. Selain itu, media sosial dapat menjadi media untuk aktualisasi diri. Akan tetapi, membagikan hal-hal detail pribadi secara real time dapat membahayakan diri pengguna dan menjadi informasi awal bagi orang lain untuk melakukan kejahatan. Ketika pengguna berbagi informasi tentang kehidupan kita sehari-hari secara real time, hal tersebut dapat memancing orang jahat untuk mengetahui keberadaan dan dengan siapa.

Selain kehilangan privasi dan keamanan data, penggunaan media sosial berlebihan dapat menyebabkan ketergantungan dan gangguan mental, celah untuk menyebarkan berita hoaks dan cyberbullying, serta mengurangi kemampuan pengguna untuk bersosialisasi. Pengguna harus membatasi penggunaan media sosial sehingga dapat mencegah dampak negatif media sosial.

Breaking News

Keamanan Siber Sosial

Rekayasa Sosial

Rekayasa sosial dalam keamanan siber adalah teknik manipulasi psikologis yang digunakan oleh peretas untuk mengeksploitasi kelemahan manusia, dengan tujuan mendapatkan akses tidak sah ke informasi atau sistem yang dilindungi.

Teknik rekayasa sosial yang sering dilakukan dengan melibatkan interaksi langsung antara penyerang dan korban. Penyerang memanfaatkan psikologi manusia untuk mengelabui target secara langsung, baik melalui panggilan telepon, tatap muka, atau komunikasi lainnya.

Teknik rekayasa sosial lainnya yang juga berbahaya yaitu penyerang menggunakan perangkat elektronik dan jaringan internet untuk mengelabui korban agar memberikan informasi atau mengunduh malware. Taktik ini biasanya menggunakan metode otomatis atau semi-otomatis, seperti email atau pesan phishing.

Teknik rekayasa sosial terakhir yang marak terjadi yaitu memanfaatkan perangkat seluler sebagai media untuk melancarkan serangan. Contoh umum teknik rekayasa sosial ini adalah Smishing (SMS Phishing). Penyerang mengirimkan pesan teks yang tampak resmi, meminta informasi pribadi atau mendesak korban untuk mengklik tautan berbahaya. Selain itu, aplikasi mobile palsu juga dapat digunakan untuk menginfeksi perangkat dengan malware.

Hukum dan Regulasi Keamanan Siber Sosial

Keamanan siber diatur dalam Perpres Nomor 47 tahun 2023 tentang strategi keamanan siber nasional dan manajemen krisis siber. Berdasarkan perpres tersebut berarti pemerintah melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial.

Pengguna sebagai warga negara Indonesia harus memiliki pengetahuan dan kepatuhan terhadap hukum dan regulasi yang mengatur keamanan siber sosial. Pengaturan keamanan siber sosial mengacu pada Undang-Undang Informasi Transaksi Elektronik, antara lain pelanggaran yang dilakukan terhadap pasal 27, pasal 28, pasal 29 dan pasal 45.

Selain itu pengguna juga dapat mengacu pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Data pribadi yang dimaksud adalah data pribadi yang bersifat spesifik dan umum. Data Pribadi yang bersifat spesifik meliputi: data dan informasi kesehatan; data biometrik; data genetika; catatan kejahatan; data anak; data keterangan pribadi; dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Sedangkan Data Pribadi yang bersifat umum meliputi: nama lengkap; jenis kelamin; agama; status perkawinan; dan/ atau Data Pribadi yang dikombinasikan mengidentifikasi seseorang.

Pengguna perlu menumbuhkan kesadaran terhadap peraturan yang berlaku. Pelanggaran terhadap hukum dan regulasi keamanan siber sosial mendapat sanksi sesuai dengan hukum dan regulasi keamanan siber sosial tersebut.

Breaking News

Keamanan Siber Sosial

Aduan Insiden Siber Sosial

Beberapa instansi pemerintah termasuk BSSN melaksanakan upaya adaptif dan inovatif dengan memberikan layanan aduan insiden siber sosial. Insiden siber sosial yang dapat dilaporkan antara lain informasi bermuatan pornografi, pelecehan dan eksploitasi seksual, pencemaran nama baik, pemerasan, berita bohong/hoaks, Suku, Agama, Ras dan Antargolongan (SARA) dan Cyberbullying.

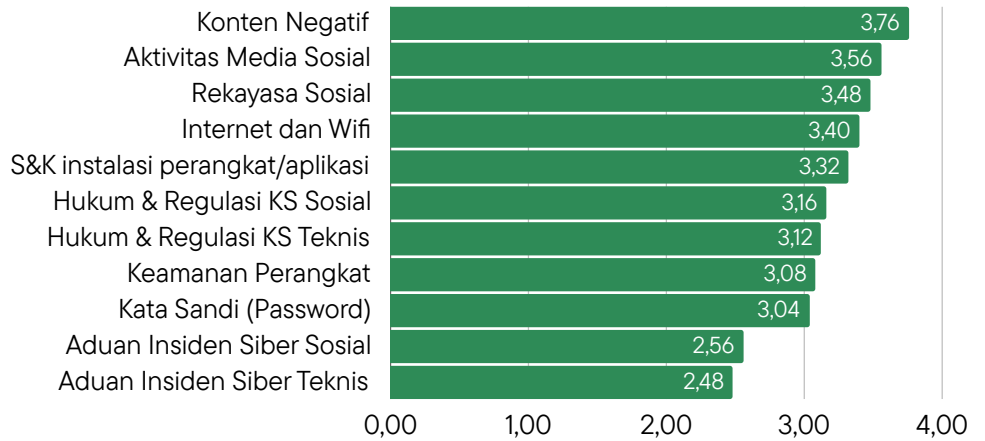
Pengguna dapat melaporkan insiden siber sosial kepada BSSN melalui alamat email: lapor.konten@bssn.go.id atau nomor telepon 081220020070. Pelapor diwajibkan mengikuti prosedur layanan aduan insiden siber sosial yang telah ditetapkan BSSN.

Selain BSSN, instansi pemerintah terkait seperti Komdigi dan Polri juga memiliki layanan aduan insiden siber sosial. Pelapor dapat memilih layanan aduan insiden siber sosial sesuai dengan kebutuhan tindak lanjut. Pelapor yang mengalami kerugian materiil dan membutuhkan penindakan dapat melapor kepada Ditipidsiber Polri. Pelapor insiden siber sosial juga harus mengikuti mekanisme pelaporan sesuai SOP layanan aduan yang diterapkan instansi pemerintah terkait.

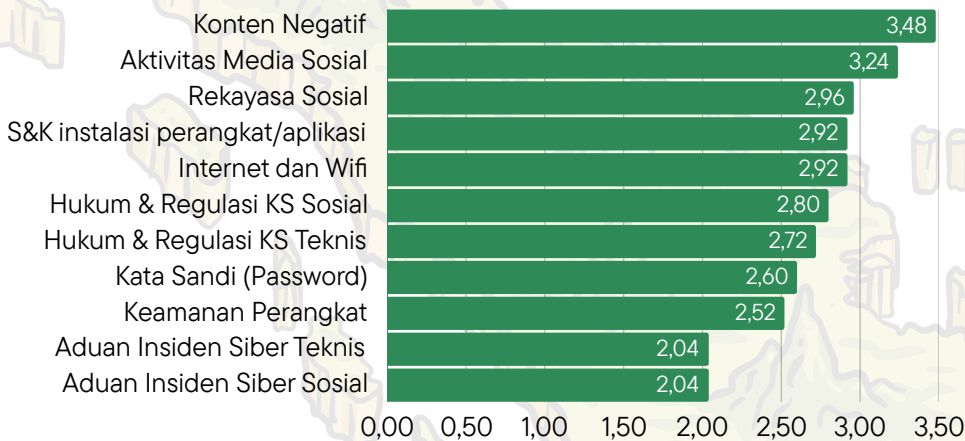


Indeks Kesadaran Keamanan Siber Provinsi

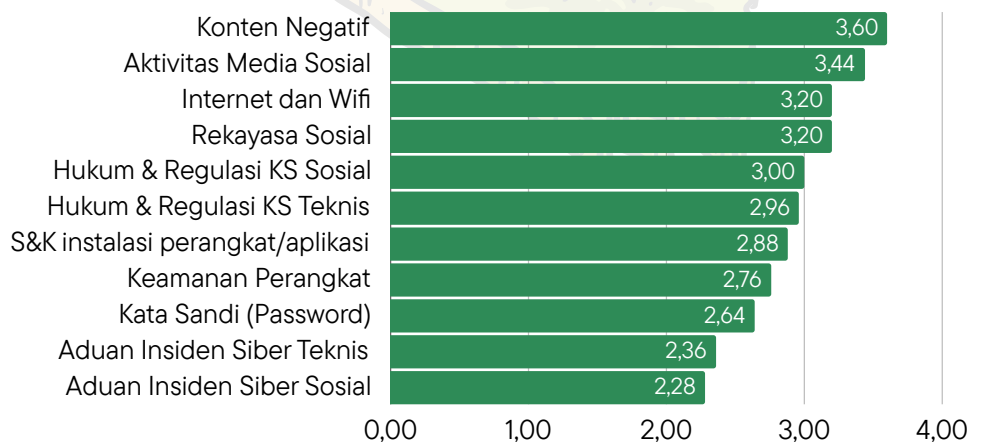
ACEH



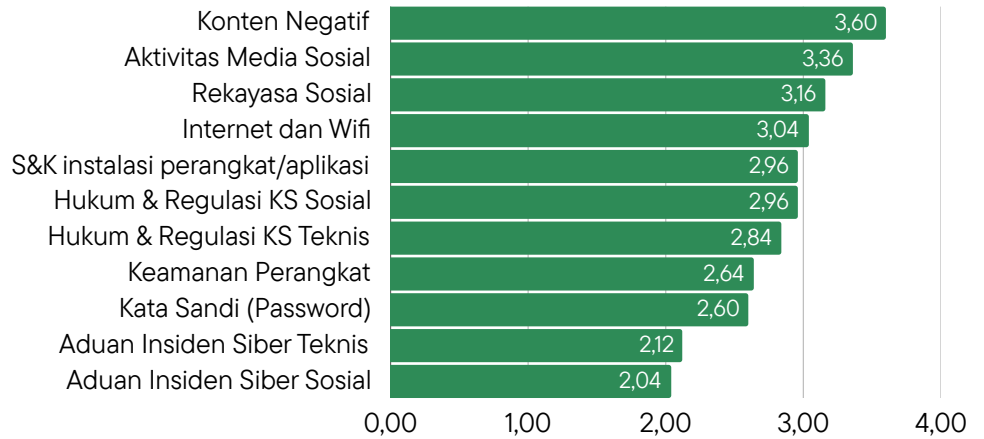
JAMBI



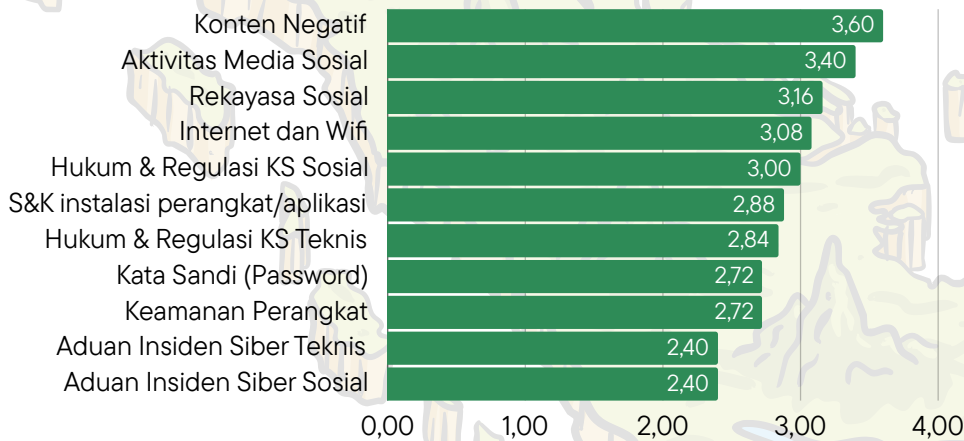
BANGKA BELITUNG



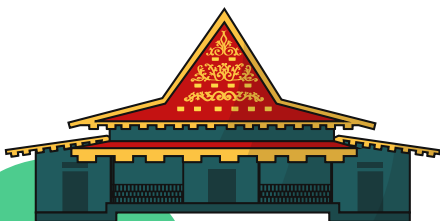
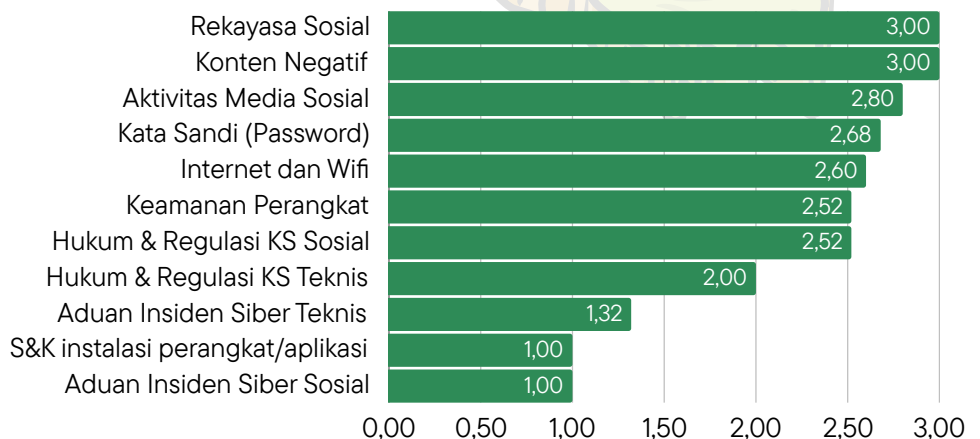
KEPULAUAN RIAU



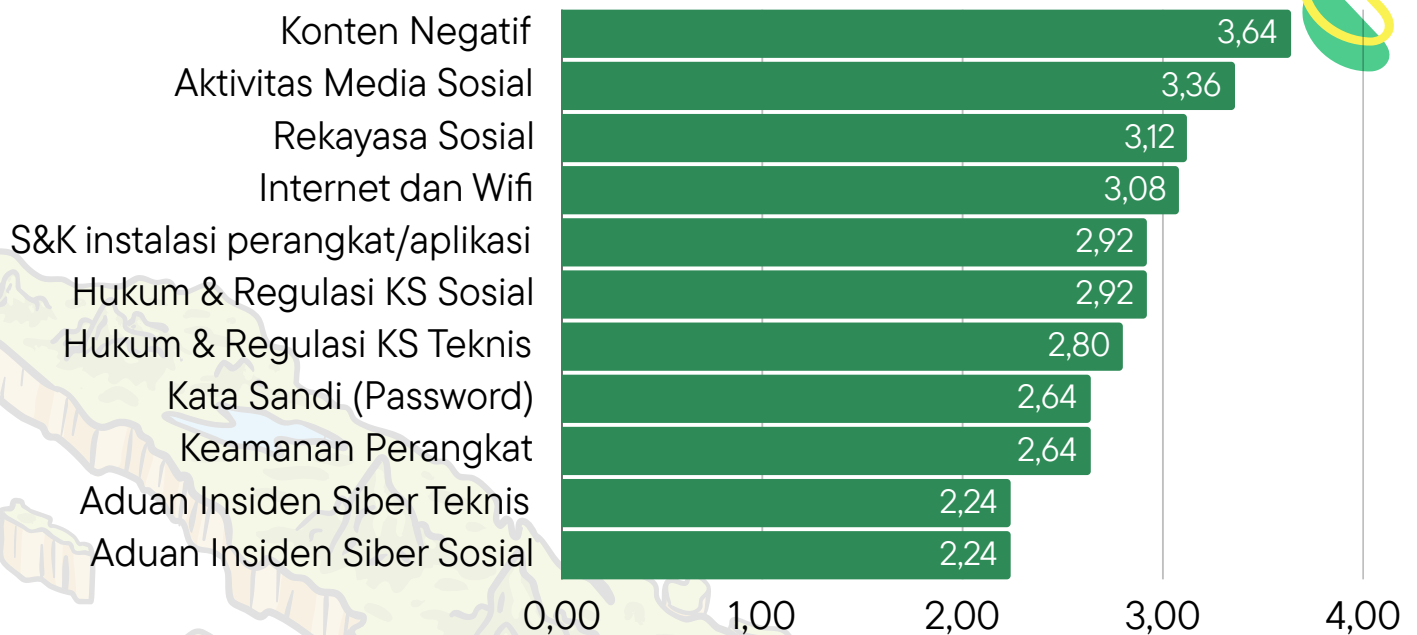
LAMPUNG



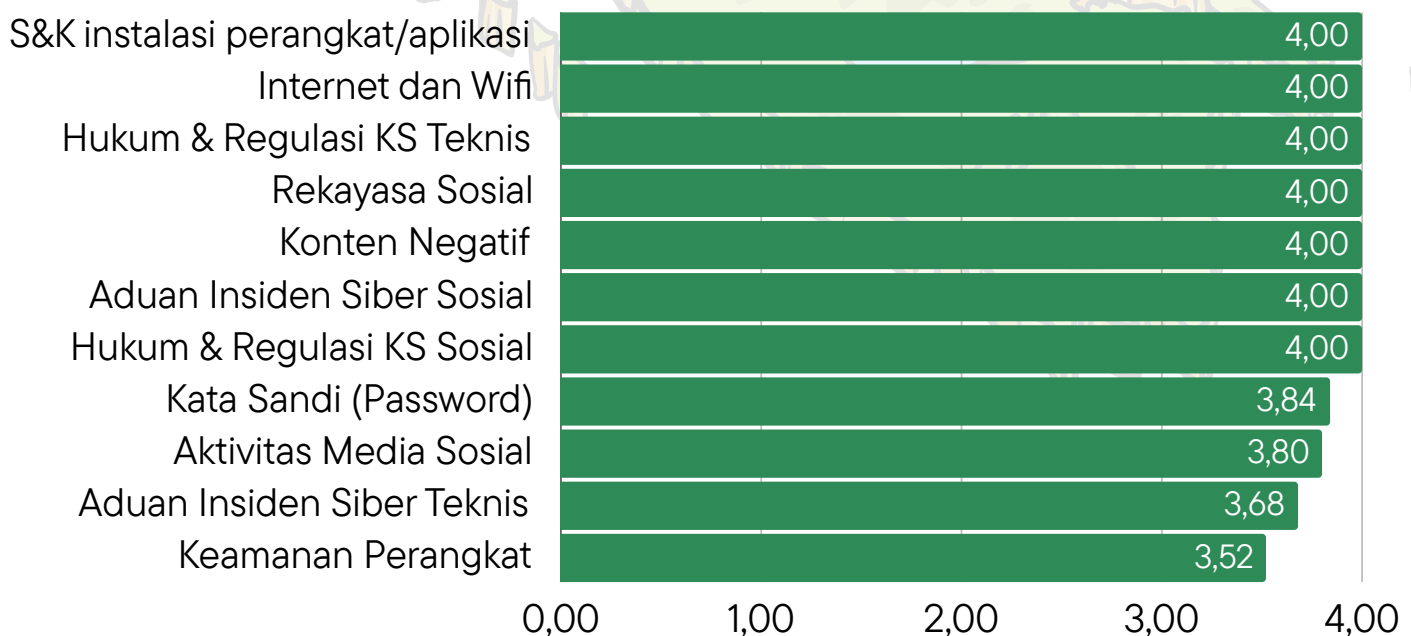
RIAU



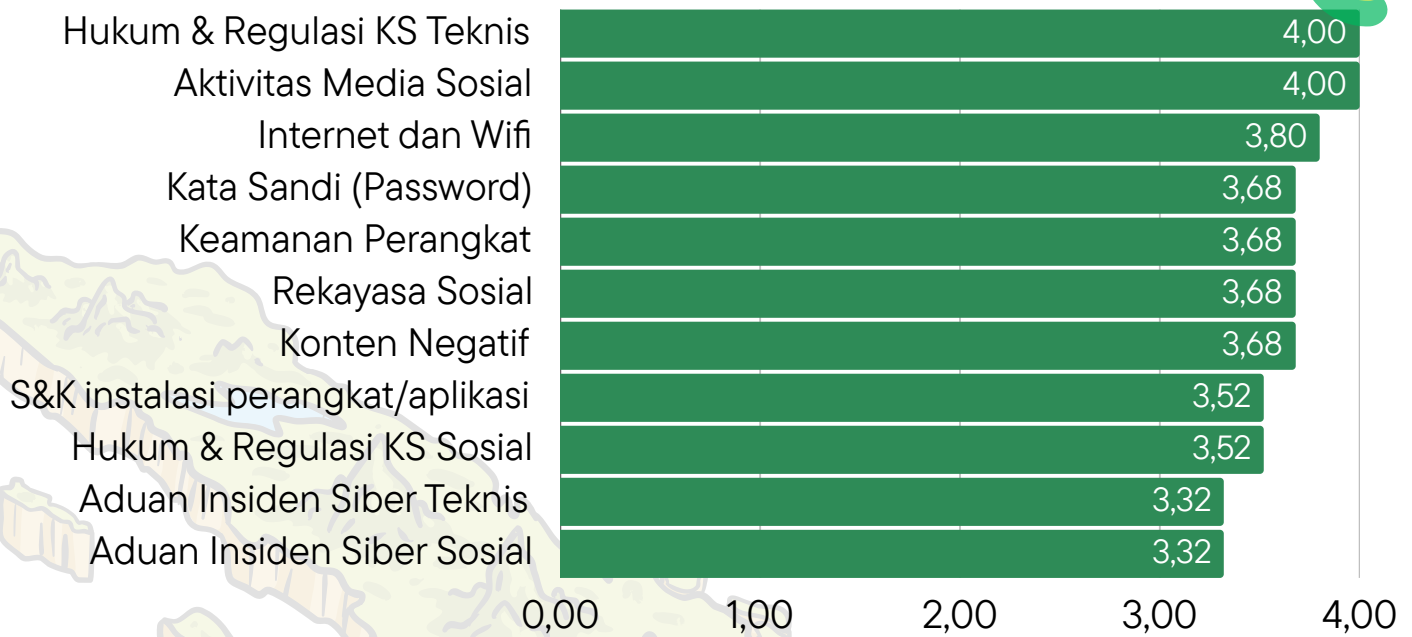
BENGKULU



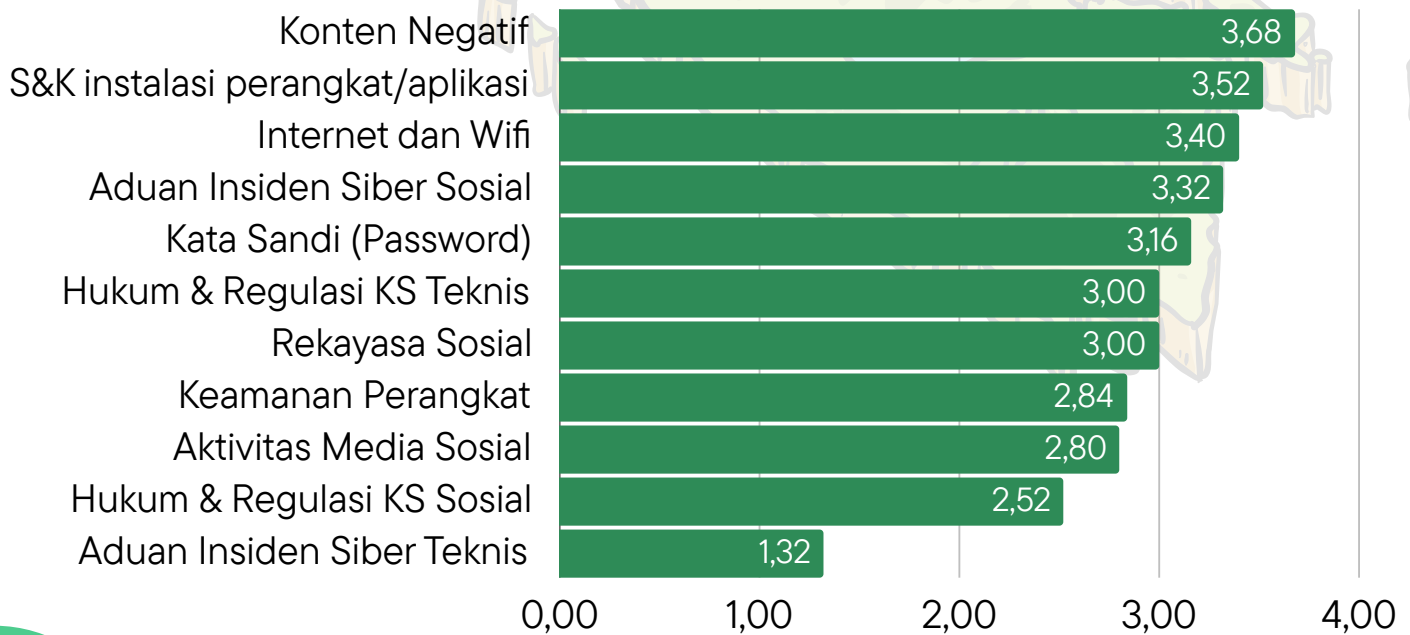
SUMATERA BARAT



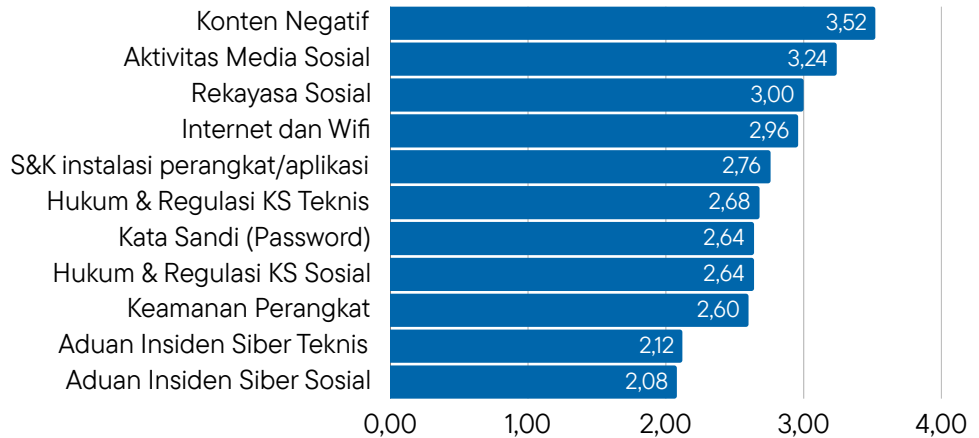
SUMATERA UTARA



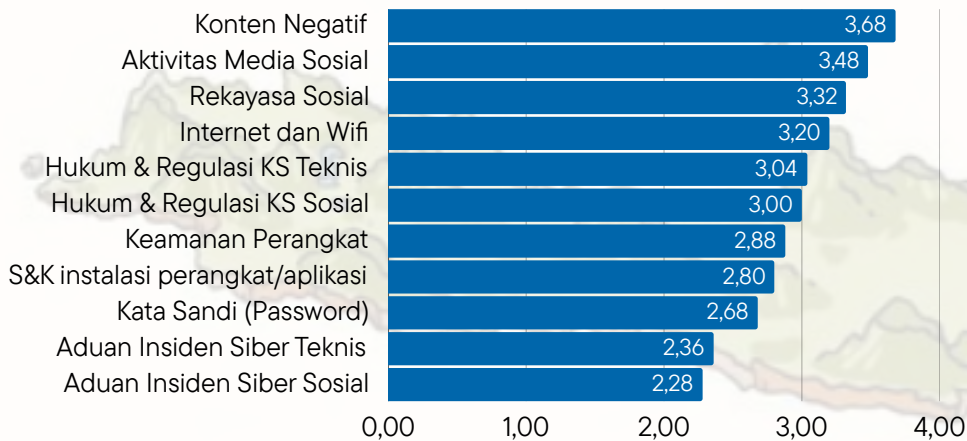
SUMATERA SELATAN



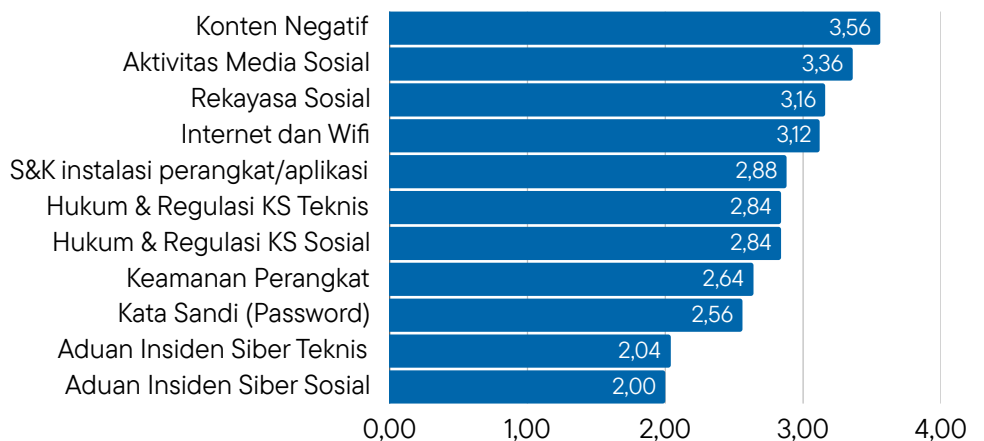
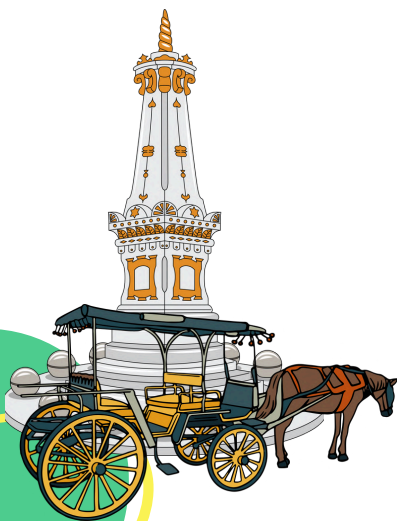
BANTEN



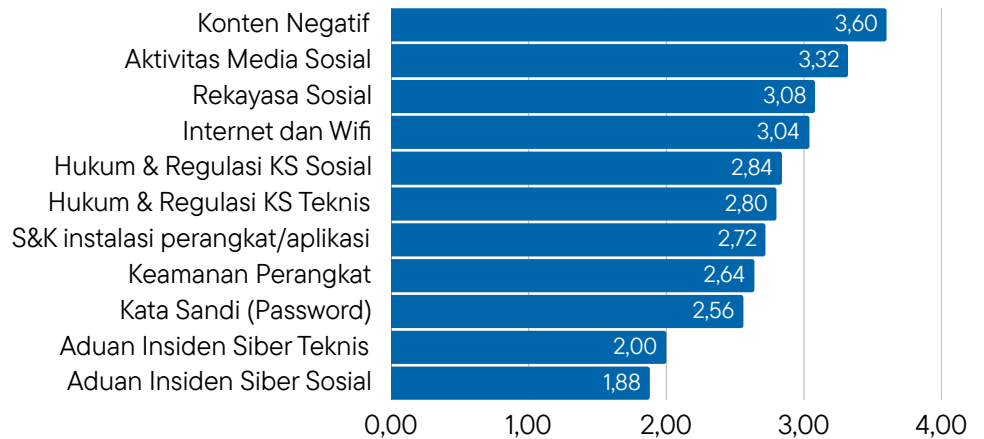
DKI JAKARTA



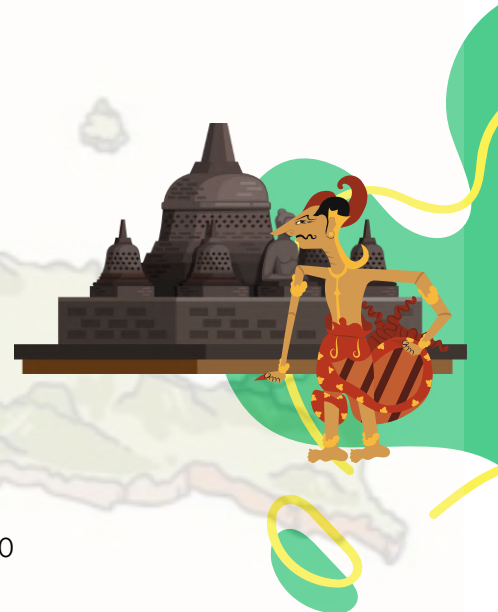
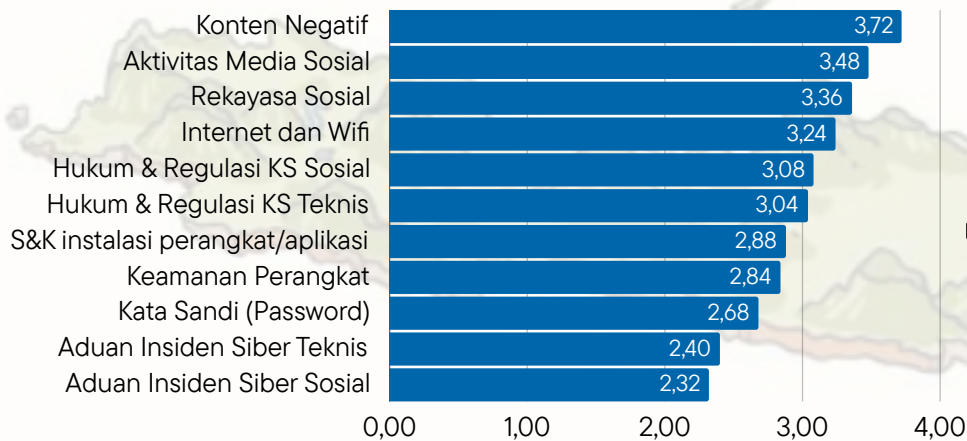
DI YOGYAKARTA



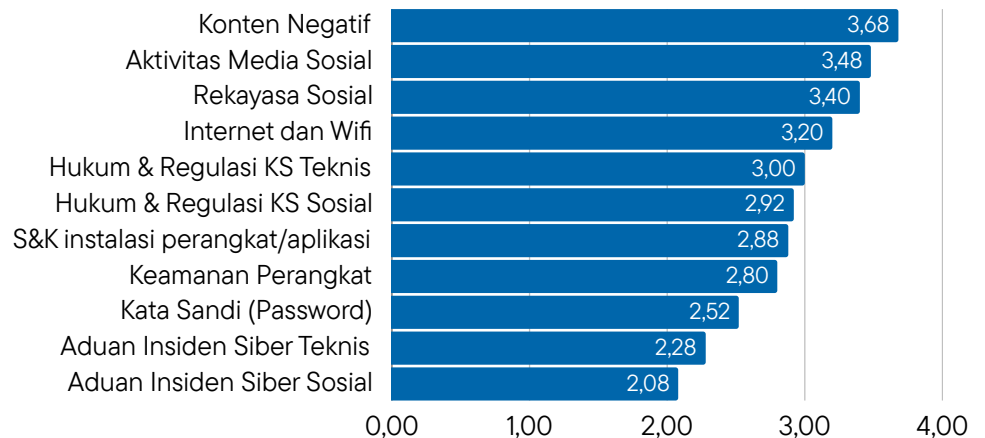
JAWA BARAT



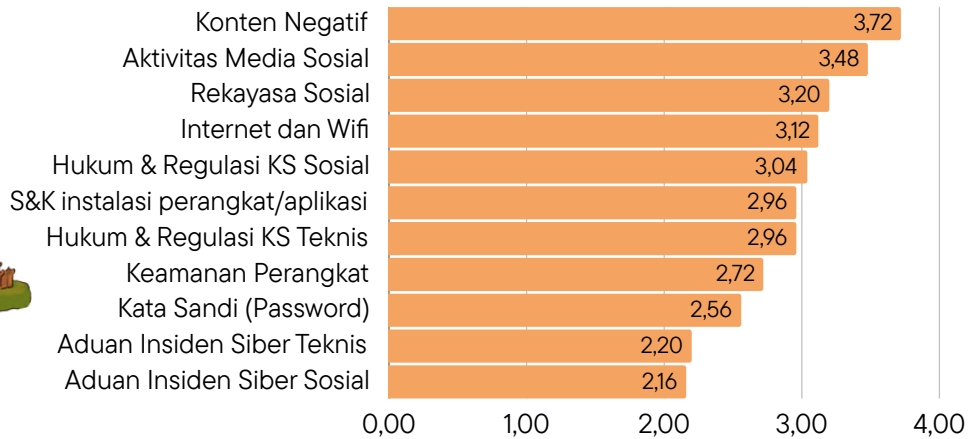
JAWA TENGAH



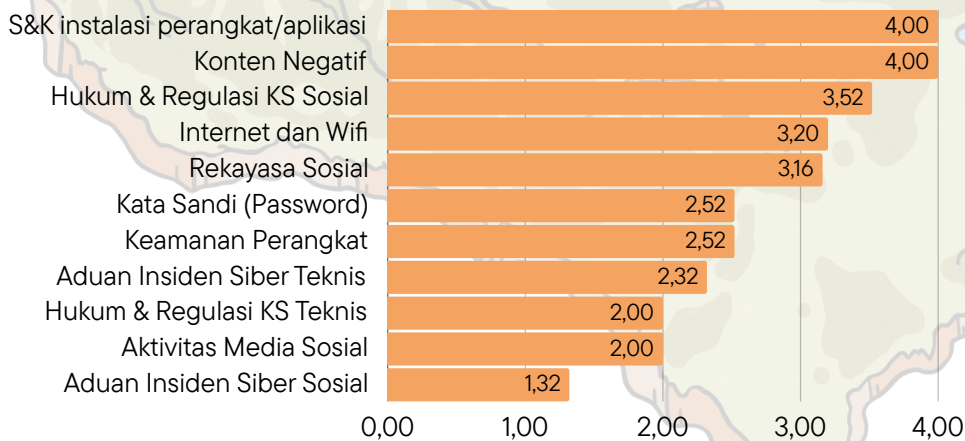
JAWA TIMUR



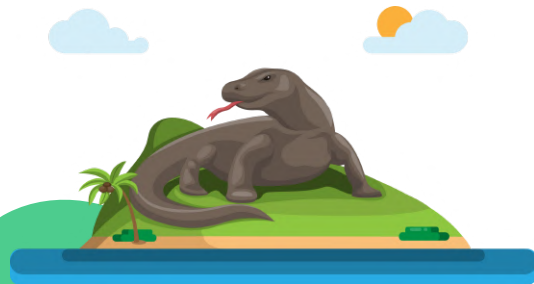
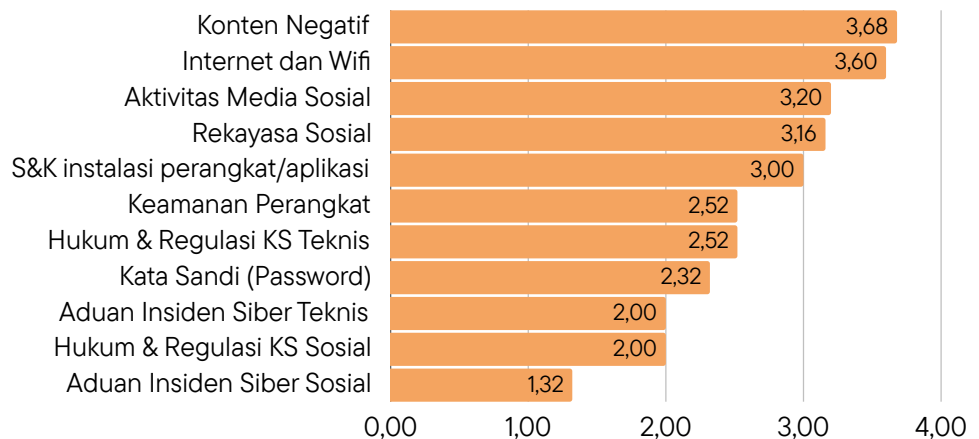
BALI



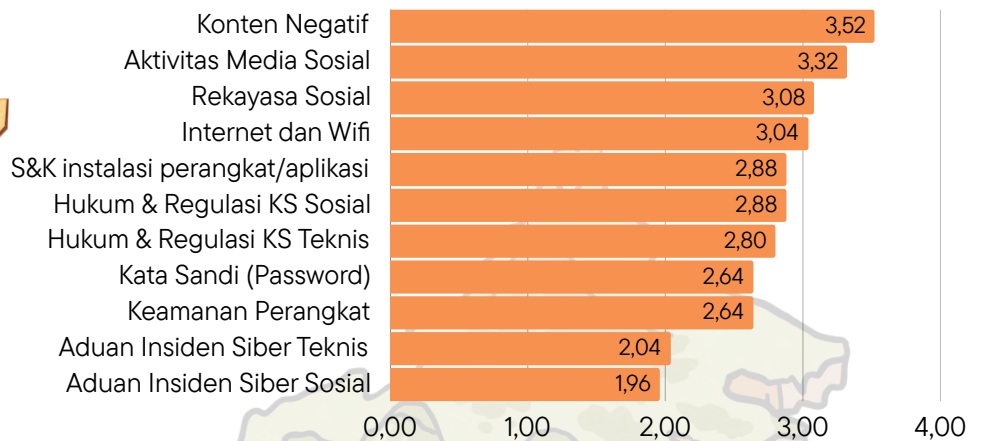
NUSA TENGGARA BARAT



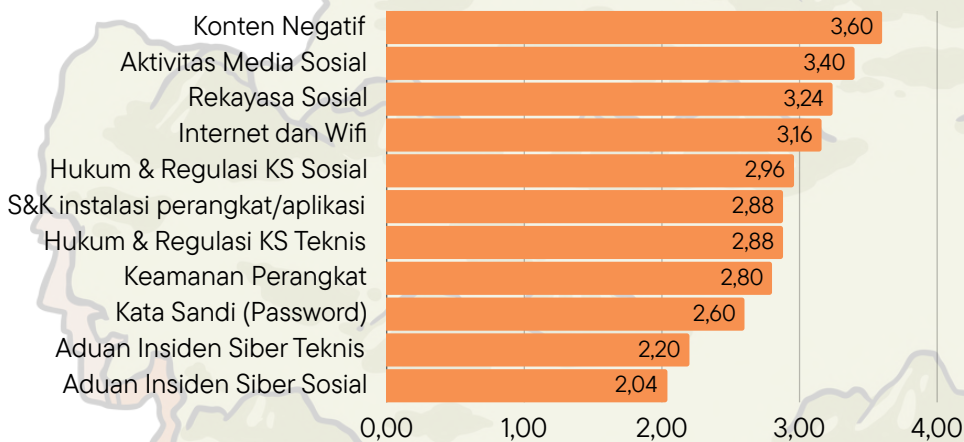
NUSA TENGGARA TIMUR



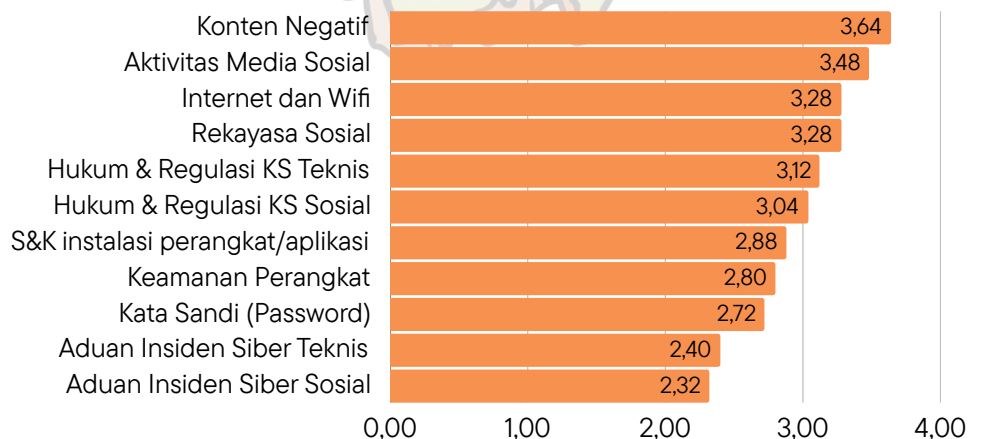
KALIMANTAN BARAT



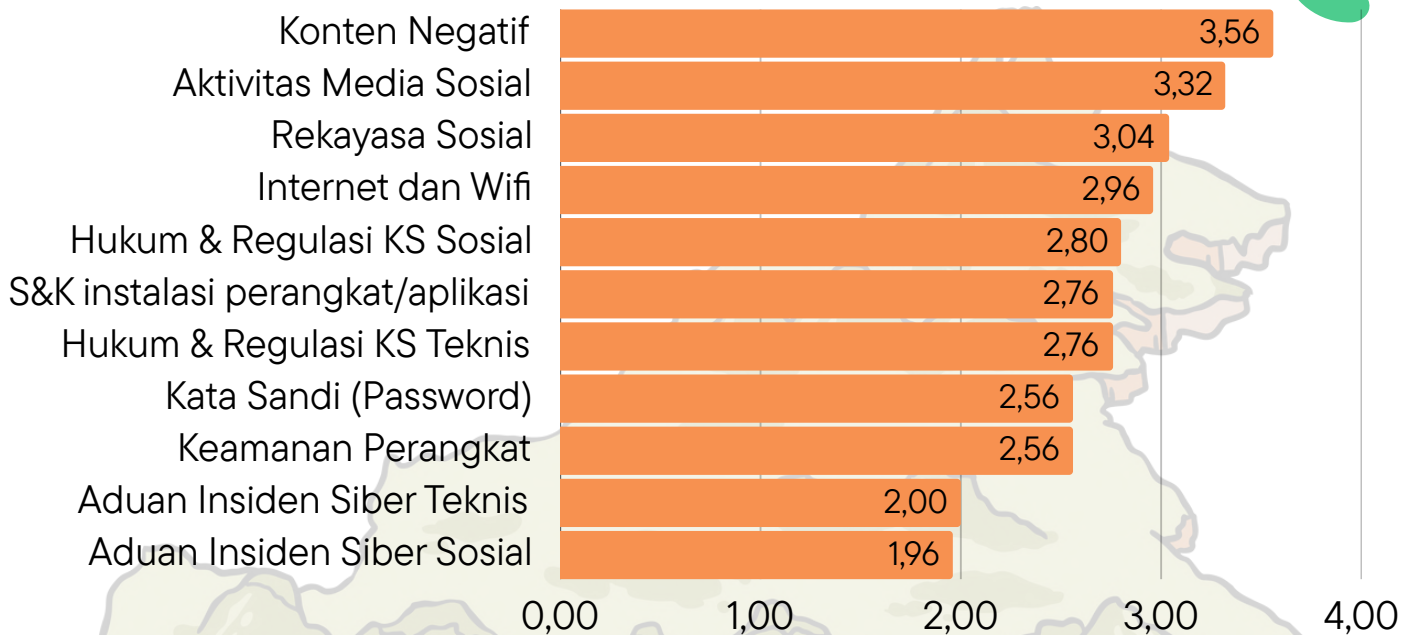
KALIMANTAN TENGAH



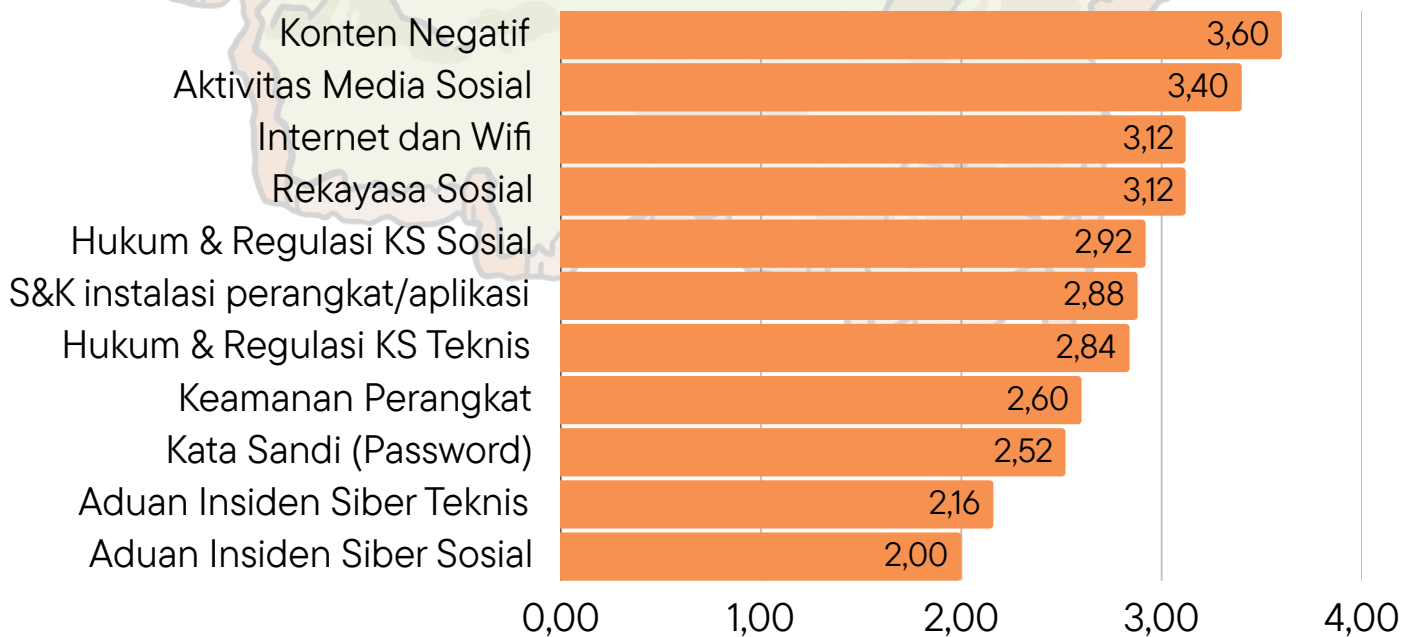
KALIMANTAN TIMUR



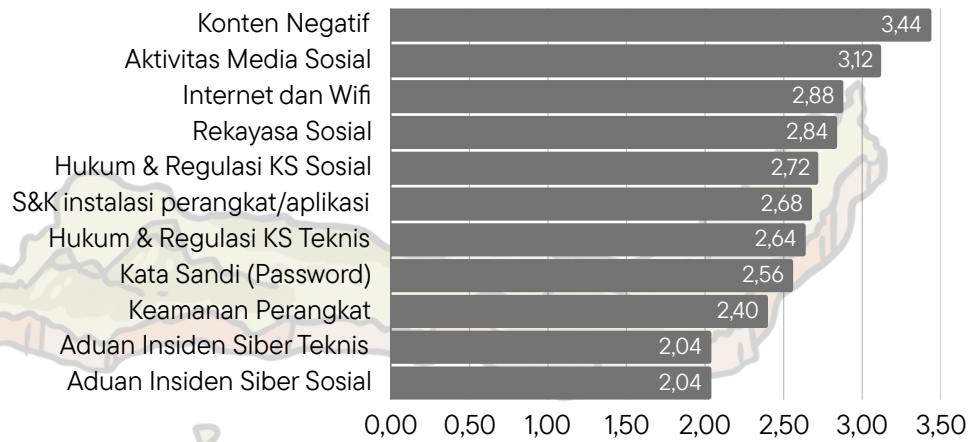
KALIMANTAN UTARA



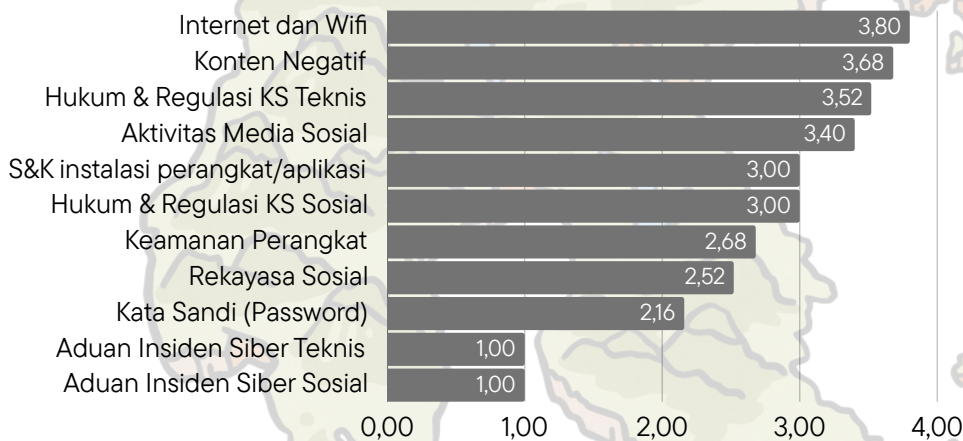
KALIMANTAN SELATAN



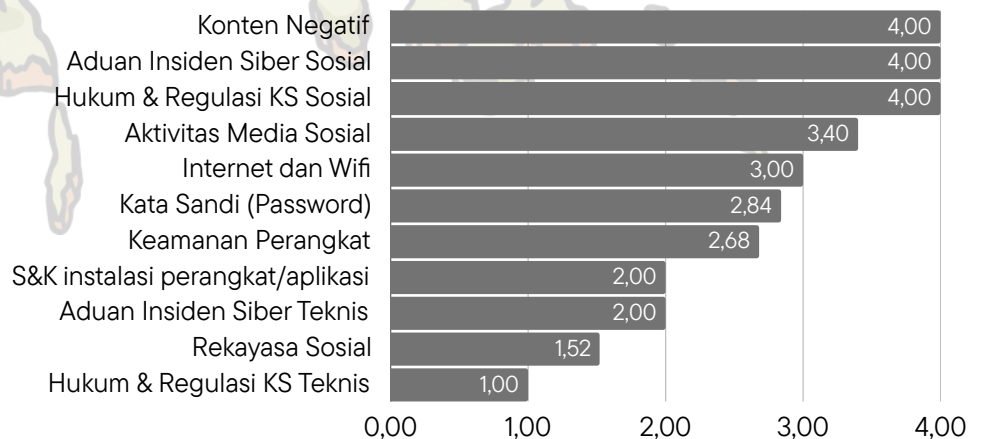
GORONTALO



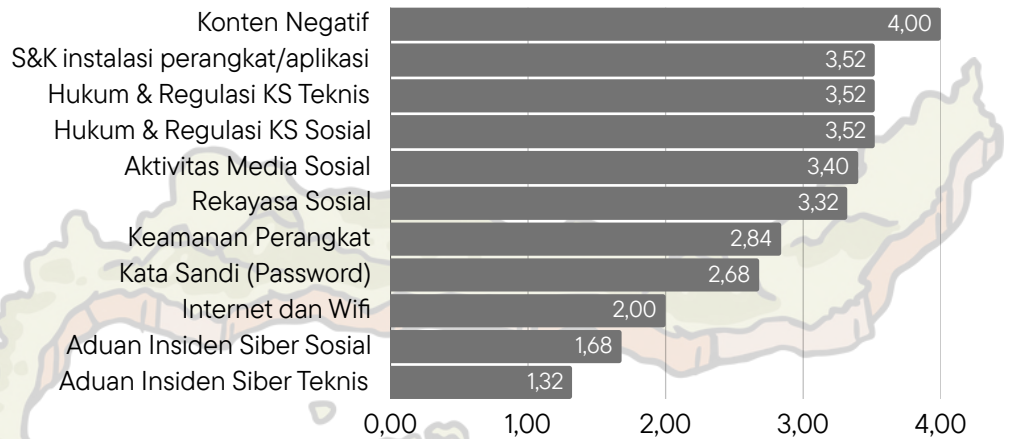
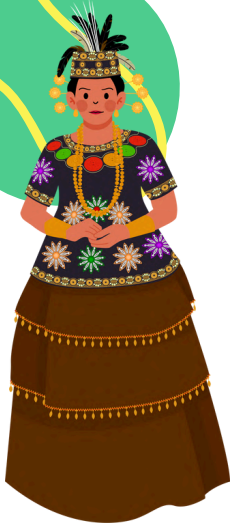
SULAWESI BARAT



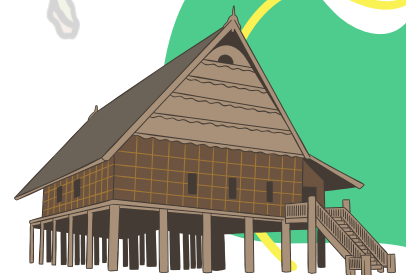
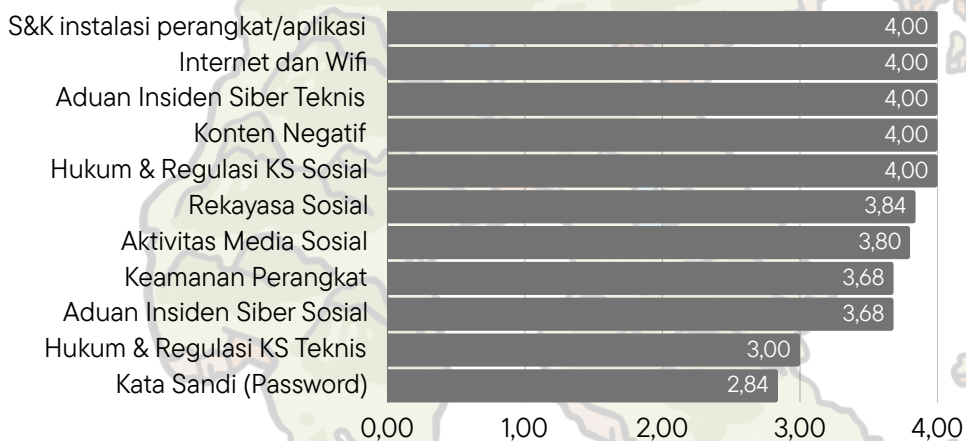
SULAWESI SELATAN



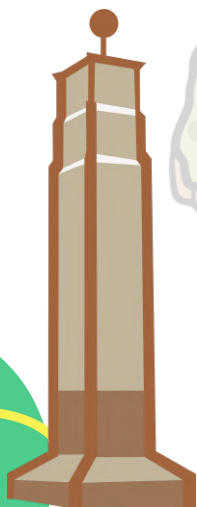
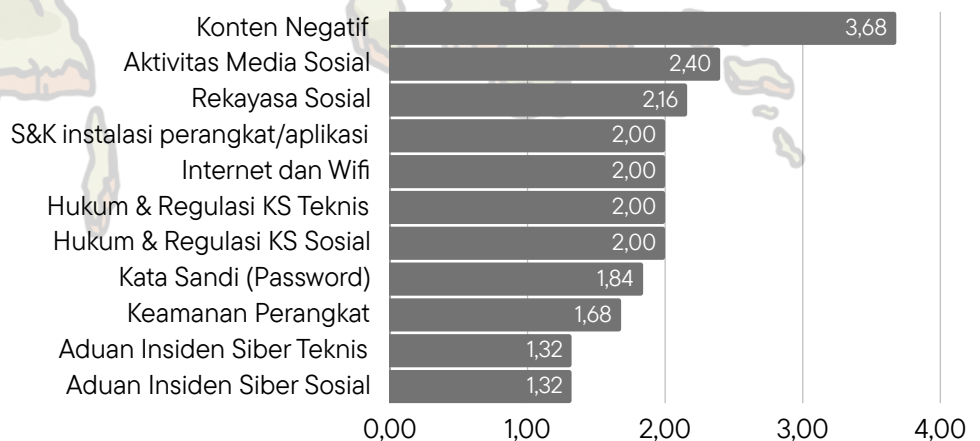
SULAWESI TENGAH



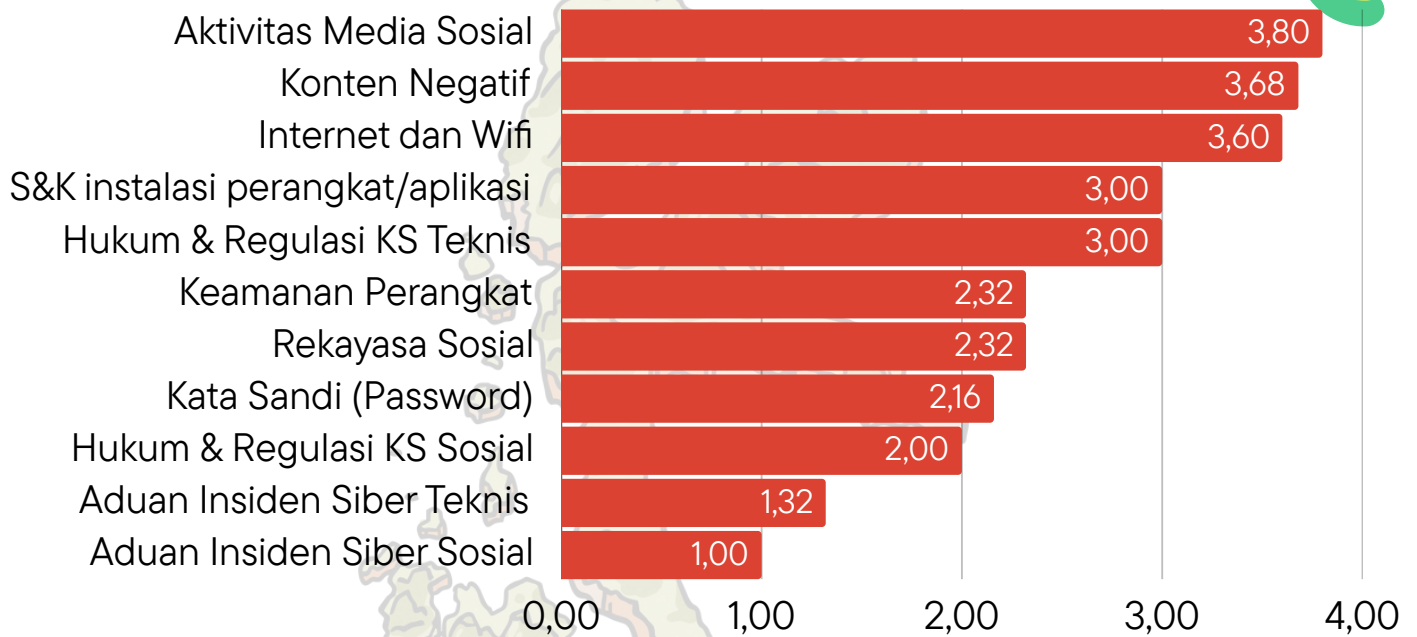
SULAWESI TENGGARA



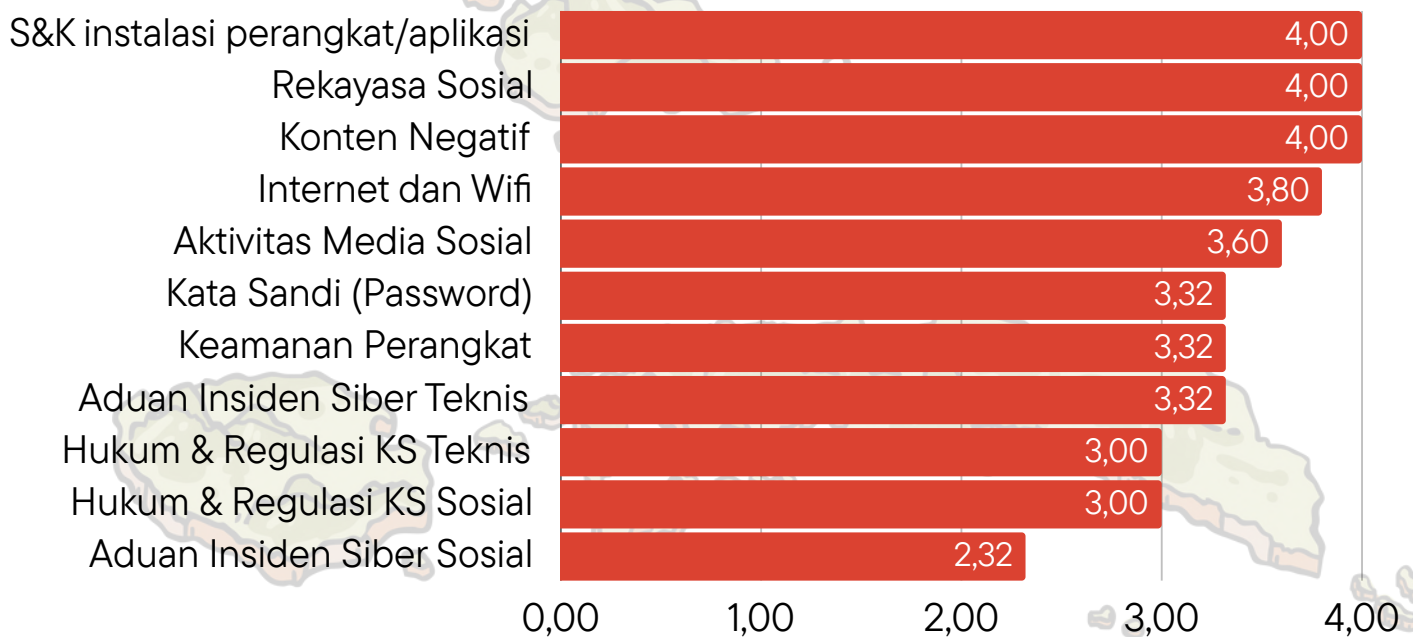
SULAWESI UTARA



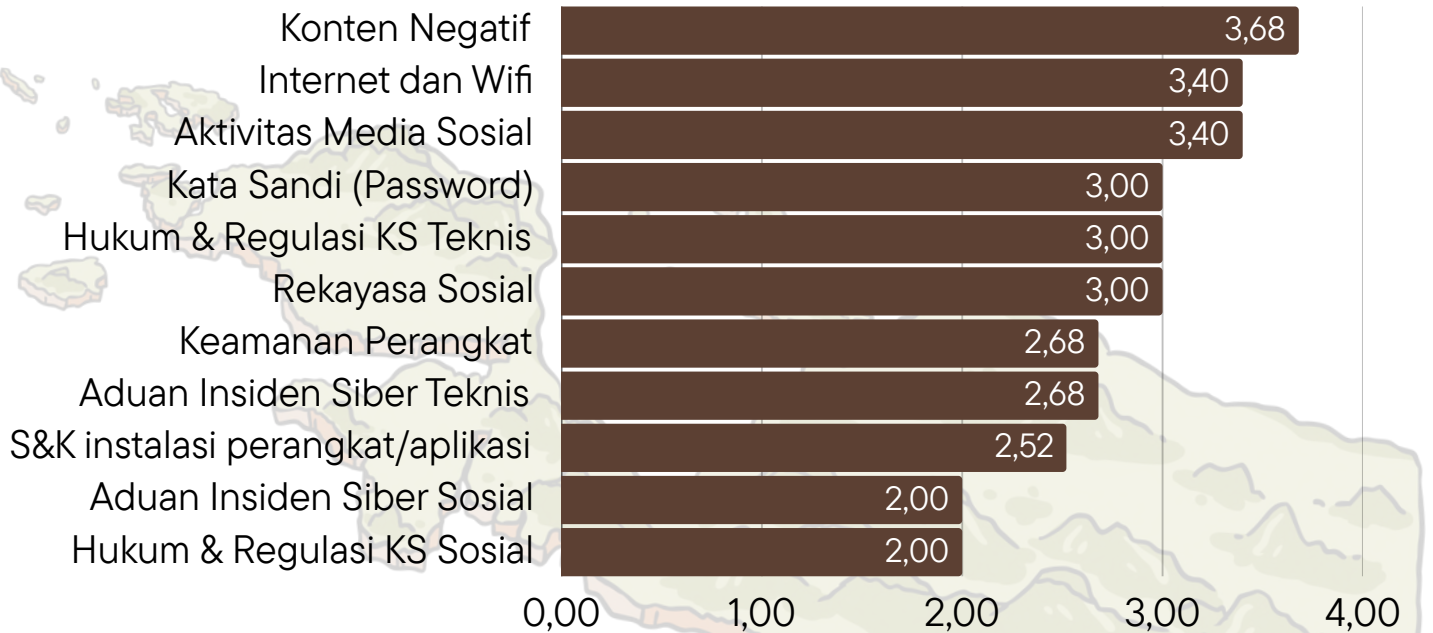
MALUKU UTARA



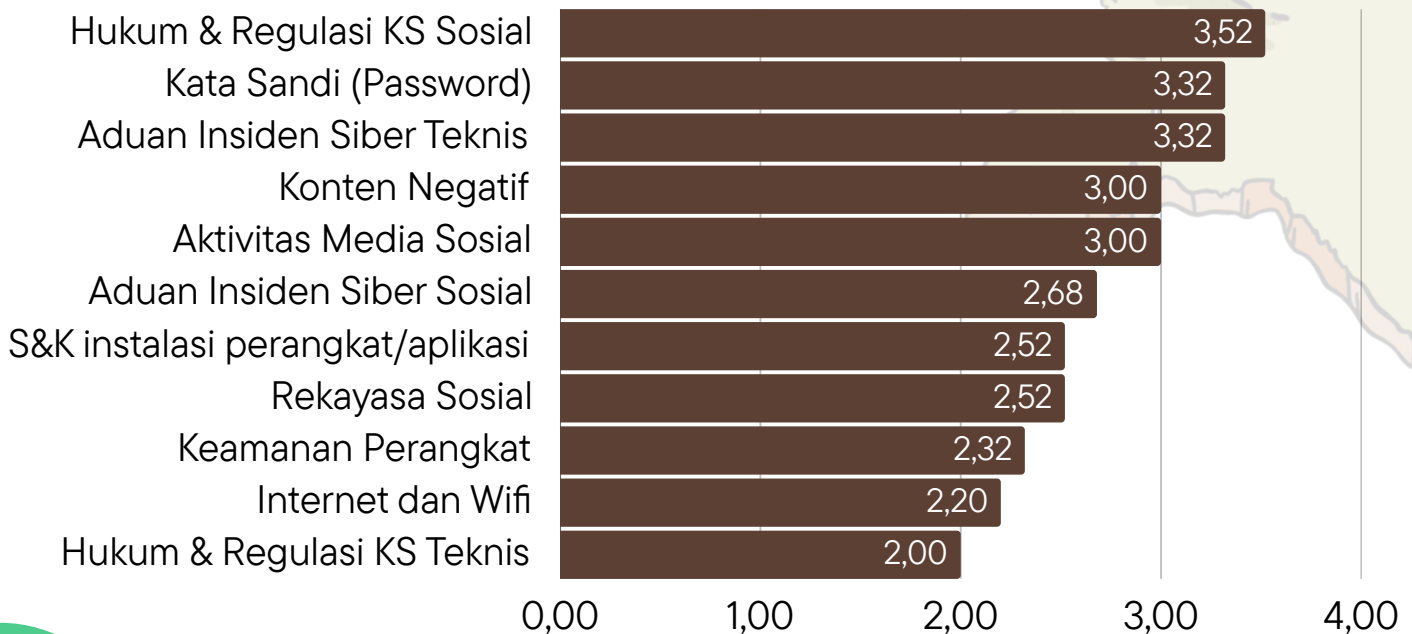
MALUKU



PAPUA



PAPUA BARAT



Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Syarat dan ketentuan instalasi perangkat/aplikasi



Grafik 4.1 Peringkat Provinsi berdasarkan Syarat dan ketentuan instalasi perangkat/aplikasi

Posisi 1: Riau (25%)

Posisi 2: Sulawesi Selatan dan Sulawesi Utara (50%)

Posisi 3: Papua dan Papua Barat (63%)

Kata Sandi (Password)



Grafik 4.2 Peringkat Provinsi berdasarkan Kata Sandi (Password)

Posisi 1: Sulawesi Utara (46%)

Posisi 2: Nusa Tenggara Timur (54%)

Posisi 3: Maluku Utara dan Sulawesi Barat (58%)

Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Internet dan Wifi



Grafik 4.3. Peringkat Provinsi berdasarkan Internet dan Wifi

Posisi 1: Sulawesi Utara (50%)
Posisi 2: Papua Barat (55%)
Posisi 3: Riau (65%)

Keamanan Perangkat



Grafik 4.4 Peringkat Provinsi berdasarkan Keamanan Perangkat

Posisi 1: Sulawesi Utara (42%)
Posisi 2: Papua Barat dan Maluku Utara (58%)
Posisi 3: Gorontalo (60%)

Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Aduan Insiden Siber Teknis



Grafik 4.5 Peringkat Provinsi berdasarkan Aduan Insiden Siber Teknis

Posisi 1: Sulawesi Barat (25%)

Posisi 2: Sumatera Selatan, Sulawesi Utara, Sulawesi Tengah, Riau, Maluku Utara (33%)

Posisi 3: Kalimantan Barat, Jambi, Gorontalo, D. I. Yogyakarta (51%)

Hukum dan Regulasi Keamanan Keamanan Siber Teknis



Grafik 4.6 Peringkat Provinsi berdasarkan Hukum dan Regulasi Keamanan Keamanan Siber Teknis

Posisi 1: Sulawesi Selatan (25%)

Posisi 2: Sulawesi Utara, Riau, Papua Barat, Nusa Tenggara Barat (50%)

Posisi 3: Nusa Tenggara Timur (63%)

Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Rekayasa Sosial



Grafik 4.7 Peringkat Provinsi berdasarkan Rekayasa Sosial

Posisi 1: Sulawesi Selatan (38%)

Posisi 2: Sulawesi Utara (54%)

Posisi 3: Maluku Utara (58%)

Konten Negatif



Grafik 4.8. Peringkat Provinsi berdasarkan Konten Negatif

Posisi 1: Papua Barat dan Riau (75%)

Posisi 2: Gorontalo (86%)

Posisi 3: Jambi (87%)

Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Aktivitas Media Sosial



Grafik 4.9 Peringkat Provinsi berdasarkan Aktivitas Media Sosial

Posisi 1: Nusa Tenggara Barat (50%)
Posisi 2: Sulawesi Utara (60%)
Posisi 3: Sumatera Selatan dan Riau (70%)

Aduan Insiden Siber Sosial



Grafik 4.10 Peringkat Provinsi berdasarkan Aduan Insiden Siber Sosial

Posisi 1: Riau, Maluku Utara, dan Sulawesi Barat (25%)
Posisi 2: Nusa Tenggara Barat dan Sulawesi Utara (33%)
Posisi 3: Sulawesi Tengah (42%)

Peringkat Provinsi berdasarkan Nilai Terendah per Variabel

Hukum dan Regulasi Keamanan Keamanan Siber Sosial



Grafik 4.11 Peringkat Provinsi berdasarkan Hukum dan Regulasi Keamanan Keamanan Siber Sosial

Posisi 1: Sulawesi Utara, Papua, Nusa Tenggara Timur, dan Maluku Utara (50%)
Posisi 2: Sumatera Selatan dan Riau (63%)
Posisi 3: Banten (66%)

KESIMPULAN



Kesimpulan

NILAI IKKS

2,855

KATEGORI NILAI
SKKS

BAIK

NILAI SUB INDIKATOR TERTINGGI

Manipulasi Data

Penyebaran Konten Negatif

Penyebaran Informasi Untuk
Menyerang Seseorang atau Kelompok
Tertentu

NILAI SUB INDIKATOR TERENDAH

Frekuensi Mengganti Password

Pengetahuan Tentang Pihak Berwenang

Kewenangan BSSN

1

Sebanyak **77,89%** responden **tidak mengganti password** akun digital mereka, baik **sama sekali (37,94%)** maupun **hanya saat teringat (39,95%)**. Kebiasaan ini berisiko, terutama bagi pelajar dengan banyak akun digital. Penting untuk meningkatkan kesadaran keamanan siber melalui kampanye literasi, seperti mengganti password secara rutin untuk mencegah serangan siber yang dapat mengancam keamanan data dan identitas.



Edukasi tentang **password manager** dan **Multi-factor Authentication (MFA)** sangat diperlukan. **Password manager** memudahkan **pengelolaan** dengan **satu password utama**, sementara **MFA** menambah keamanan melalui **verifikasi tambahan**, seperti **OTP** atau **biometrik**. Simulasi serangan siber juga efektif, memberikan pengalaman langsung tentang dampak serangan dan cara menanggulangnya, seperti mengenali phishing atau mengamankan perangkat dari malware.

2

3

Sebanyak **50,33%** responden **tidak mengetahui** pihak berwenang yang dapat dihubungi saat mengalami insiden siber, sementara hanya **12,70%** yang **mengetahui** cara melaporkannya. Hal ini menunjukkan **mayoritas pelajar kurang memahami** langkah yang tepat saat menghadapi **insiden siber**. Akibatnya, penanganan masalah bisa tertunda, memperparah dampak seperti pencurian atau penyalahgunaan data pribadi.

Kampanye edukasi tentang pihak berwenang yang menangani insiden siber menjadi langkah **penting**. Integrasi materi keamanan siber, termasuk cara melaporkan insiden, ke dalam mata pelajaran seperti **TIK** atau **PPKn**, dapat meningkatkan kesadaran pelajar sejak dini. Dengan pendekatan ini, diharapkan pelajar lebih siap menghadapi ancaman siber.



Sebanyak **50,06%** responden **tidak mengetahui** bahwa **Badan Siber dan Sandi Negara (BSSN)** memiliki **layanan aduan siber**, sementara hanya **13,38%** yang **memahami mekanisme pelaporannya**. Mayoritas pelajar tidak menyadari peran BSSN dalam menangani kasus siber, sehingga mereka rentan terhadap insiden seperti peretasan akun dan penyalahgunaan data pribadi.

4



Untuk meningkatkan kesadaran, diperlukan **kampanye edukasi nasional** yang memperkenalkan **BSSN** sebagai **lembaga berwenang dalam pengaduan siber**. Kampanye ini dapat dilakukan melalui **media sosial, situs sekolah, dan media massa**. Selain itu, materi keamanan siber dan prosedur pelaporan ke BSSN perlu diintegrasikan dalam pelajaran sekolah, seperti TIK dan PPKn.



Informasi layanan aduan BSSN juga dapat disebarkan melalui **platform e-learning** yang sering digunakan siswa. Kerja sama BSSN dengan sekolah untuk memberikan pelatihan dasar keamanan siber akan memperkuat pemahaman pelajar tentang pentingnya melaporkan insiden siber dan meningkatkan kesiapan mereka menghadapi ancaman.

DAFTAR PUSTAKA

American Academy of Pediatrics. 2023. The Effects of Social Media on Teen Mental Health: Trends and Concerns. American Academy of Pediatrics, Volume 151, Issue 5.

Anderson, J., et al. (2022). Technical Cybersecurity: A Comprehensive Overview. Journal of Cybersecurity, 18(4), 243-257.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). 2022. Survei terkini Jumlah Pengguna Internet Indonesia. Jakarta

Awaliyah, C., Dewi, D. A., & Furnamasari, Y. F. 2021. Media Sosial Mempengaruhi Integrasi Bangsa. ISSN: 2614-3097, Vol.5 No.3.

Bonneau, J., et al. (2023). The Efficacy of Two-Factor Authentication. International Journal of Information Security, 22(3), 201-213.

Cyberpsychology, Behavior, and Social Networking. 2023. Mapping Adolescent Cybersecurity Behavior for Effective Digital Literacy Programs. Cyberpsychology Journal, Volume 26, Issue 4, pp. 211-220

Das, R., et al. (2022). Password Security in Digital Natives. Computers & Security, 34(5), 305-321.

Doni, F. R. 2017. Perilaku Penggunaan Media Sosial Pada Kalangan Remaja. IJSE – Indonesian Journal on Software Engineering, Vol.3 No.2.

Drakel, W. J. 2018. Perilaku Mahasiswa Dalam Menggunakan Media Sosial di Universitas Sam Ratulangi Manado. Holistik, Vol.11 No.21A.

Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. 1994. Cyberspace and the american dream: A magna carta for the knowledge age, future insight.

Hadlington, L. (2023). Social Engineering Risks Among High School Students. European Journal of Cybersecurity Research, 12(2), 89-101.

DAFTAR PUSTAKA

Indonesia. 2003. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang. Sekretariat Negara. Jakarta.

Indonesia. 2016. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sekretariat Negara. Jakarta.

Indonesia. 2018. Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang. Sekretariat Negara. Jakarta.

Indonesia. 2023. Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Sekretariat Negara. Jakarta.

Jagatic, T. N., et al. (2022). Phishing Attacks and Their Psychological Impact on Adolescents. *Cyberpsychology Journal*, 29(3), 157-171.

Kementerian Komunikasi dan Informatika (KOMINFO). 2024. Survei Nasional Penggunaan Media Sosial di Kalangan Pelajar. Jakarta: Kementerian Komunikasi dan Informatika.

Peraturan Badan Siber dan Sandi. 2021. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara. Jakarta.

Peraturan Badan Siber dan Sandi Negara. 2018. Peraturan Badan Siber dan Sandi Negara Nomor 3 Tahun 2018 tentang Sistem Nilai Badan Siber dan Sandi Negara. Jakarta. Peraturan Badan Siber dan Sandi. 2022.

Peraturan Badan Siber dan Sandi Negara. 2023. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Pelatihan Keamanan Siber dan Persandian. Jakarta.

Badan Siber dan Sandi Negara

DAFTAR PUSTAKA

Peraturan Badan Siber dan Sandi. 2022. Peraturan BSSN Nomor 8 Tahun 2022 tentang Pemberdayaan Keamanan Siber dan Ketahanan Sektor Pendidikan. Jakarta.

Peraturan Badan Siber dan Sandi. 2024. Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028. Jakarta.

Peraturan Presiden. 2021. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Sekretariat Negara. Jakarta.

Suryani, I., Liliyana, Handar, M., & Ekasuci, R. 2020. Pemanfaatan Media Sosial Sebagai Media Promosi Bagi Radio Mersi 93.9 FM. Journal Komunikasi, Vol.11 No.1.

UNESCO. 2024. Youth in Digital Spaces: Exposure to Harmful Content and the Need for Online Safety. UNESCO Digital Report Series.