

Studi Pengaruh Kesadaran Keamanan Siber Terhadap Kepercayaan Pengguna dalam Menggunakan SIAKAD Esa Unggul dengan Metode Analisis Deskriptif Kuantitatif

Samuel Mahesa Sinulingga^{1✉}, Jesen Candra², Johta Sansanda Suntana³, Gifaren Permana⁴, Farrel Reyhan Putra⁵, Dewi Setiowati⁶

sinulingga848@student.esaunggul.ac.id¹, jesencandra123@student.esaunggul.ac.id²,

suntana1101@student.esaunggul.ac.id³, gifaren12@student.esaunggul.ac.id⁴,

sunmgaming@student.esaunggul.ac.id⁵, dewi.setiowati@esaunggul.ac.id⁶

^{1,2,3,4,5,6} Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul, Indonesia

Keywords: Kesadaran Keamanan Siber, Kepercayaan Pengguna, Portal Akademik, SIAKAD Esa Unggul, Survei Kuantitatif	Abstrak
Submitted: dy/mn/year	Studi ini menelaah korelasi antara tingkat literasi keamanan digital dengan keyakinan pengguna pada sistem informasi akademik (SIAKAD) di lingkungan Universitas Esa Unggul. Dalam era digital yang penuh ancaman siber, pemahaman dan kewaspadaan pengguna menjadi aspek krusial. Melalui pendekatan deskriptif kuantitatif, data dikumpulkan menggunakan kuesioner Google Form dari mahasiswa pengguna aktif SIAKAD. Riset ini bertujuan untuk menilai level pemahaman mahasiswa mengenai keamanan digital, kemudian menganalisis hubungannya dengan keyakinan mereka pada keandalan sistem. Hasil awal menunjukkan adanya hubungan antara pengetahuan tentang ancaman siber, praktik aman berinternet, dan tingkat kepercayaan pada perlindungan data di SIAKAD. Temuan ini mengidentifikasi area yang membutuhkan peningkatan kesadaran, yang berpotensi memperkuat kepercayaan pengguna serta meningkatkan keamanan digital kampus. Riset ini ditutup dengan rekomendasi intervensi edukatif untuk membentuk budaya digital yang aman dan terpercaya di lingkungan Universitas Esa Unggul.
Revised: dy/mn/year	
Accepted: dy/mn/year	
Corresponding Author: Samuel Mahesa Sinulingga Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul, Indonesia Jakarta, Indonesia Email: sinulingga848@student.esaunggul.ac.id	

PENDAHULUAN

Dunia pendidikan tinggi kini tak bisa lepas dari jerat teknologi; Sistem Informasi Akademik atau yang akrab disebut SIAKAD telah menjadi tulang punggung operasional berbagai kampus, termasuk Universitas Esa Unggul. Bayangkan saja, SIAKAD ini

layaknya jantung digital yang memompa aliran data akademik, mulai dari jadwal kuliah, nilai, hingga informasi personal mahasiswa dan dosen. Walaupun menawarkan berbagai keunggulan dalam hal akses dan efektivitas, sistem ini juga menyimpan potensi kerentanan terhadap berbagai ancaman di dunia maya. Tak bisa dipungkiri, berita tentang kebocoran data atau serangan siber yang melumpuhkan sistem sudah sering kita dengar, dan hal ini tentu saja menggerogoti rasa aman dan kepercayaan pengguna terhadap sistem yang mereka andalkan. Kepercayaan ini menjadi sangat vital, sebagaimana pengaruh *cyber crime* dan *cyber security* juga signifikan terhadap tingkat kepercayaan nasabah dalam menggunakan layanan digital perbankan di wilayah Surabaya (Febriana & Indrarini, 2024).

Isu mengenai kepercayaan pengguna ini mengemuka sebagai aspek yang sangat penting, terutama jika dikaitkan dengan tingkat pemahaman akan keamanan siber (*cybersecurity awareness*) di kalangan pengguna, terlebih lagi pada kelompok mahasiswa yang dominan dalam penggunaan SIAKAD. Ibaratnya, secanggih apapun gembok yang dipasang, jika penghuni rumah tidak peduli dengan keamanan, pintu rumah tetap saja bisa terbuka lebar bagi ‘tamu tak diundang’. Banyak penelitian menunjukkan bahwa tingkat "melek" keamanan siber ini seringkali tidak optimal. Ini terlihat dalam studi seperti yang dilakukan oleh Nurdin dan Rahman (2023) mengenai pengukuran tingkat kesadaran keamanan siber pengguna media sosial di kalangan mahasiswa teknik informatika, atau yang dilakukan oleh Faliandy et al. (2023) tentang analisis kesadaran pengguna aplikasi e-Court di lingkungan pengadilan. Bahkan, penelitian oleh Khando et al. (2021) secara komprehensif mengulas pentingnya meningkatkan kesadaran keamanan informasi karyawan di berbagai organisasi, baik swasta maupun publik, yang menunjukkan betapa universalnya isu ini. Hal ini sejalan dengan temuan Mahendra et al. (2024) yang menyoroti tingkat kesadaran keamanan cyber di media sosial Instagram pada siswa SMK, yang notabene merupakan generasi digital natif.

Meskipun telah banyak penelitian yang mengupas tentang kesadaran keamanan siber, seperti peran mahasiswa dalam peningkatannya di lingkungan kampus (Jasmine et al., 2025) atau studi pada kalangan mahasiswa universitas di Kota Batam (Adzkia et al., 2024), namun kajian yang secara spesifik menjahit benang merah antara kesadaran keamanan siber mahasiswa dengan tingkat kepercayaan mereka terhadap SIAKAD di lingkungan Universitas Esa Unggul masih menjadi area yang menarik untuk digali lebih dalam. Keunggulan riset ini adalah pendekatannya dalam mengevaluasi secara kuantitatif bagaimana pengetahuan dan pandangan mahasiswa mengenai keamanan siber berhubungan dengan tingkat kepercayaan yang mereka rasakan selama menggunakan SIAKAD. Dengan memahami relasi ini, diharapkan dapat dirumuskan strategi jitu untuk tidak hanya meningkatkan kesadaran, tetapi juga membangun benteng kepercayaan yang kokoh, sebagaimana pentingnya sistem pengamanan file dan *cyber security* pada pengamanan objek vital PT PDAM (Soesanto et al., 2023). Pada akhirnya, optimasi *cyber security* seperti yang diupayakan pada sistem *e-government* oleh Y. W. et al. (2025) menjadi tujuan yang ingin dicapai demi integritas dan kenyamanan seluruh pengguna SIAKAD.

METODOLOGI PENELITIAN

Kami menggunakan metode survei untuk melakukan analisis deskriptif kuantitatif dalam penelitian ini. Pendekatan ini dipilih untuk memberikan gambaran yang jelas dan terukur mengenai fenomena pengaruh kesadaran keamanan siber terhadap kepercayaan pengguna SIAKAD Esa Unggul, serupa dengan pendekatan kuantitatif yang digunakan dalam studi optimasi keamanan siber pada sistem *e-government* (Y. W. et al., 2025) dan juga sejalan dengan metode survei yang diterapkan oleh Faliandy et al. (2023) dalam menganalisis kesadaran keamanan siber pengguna aplikasi e-Court. Tujuannya adalah untuk memotret dan menjelaskan fenomena tersebut secara apa adanya berdasarkan angka-angka yang terkumpul.

Desain Penelitian dan Subjek Penelitian

Rancangan studi ini mengadopsi pendekatan survei deskriptif dengan orientasi kuantitatif, yang dimaksudkan untuk mengenali serta memaparkan bagaimana kesadaran akan keamanan siber mempengaruhi tingkat kepercayaan pengguna terhadap SIAKAD. Pengumpulan data awal dilakukan melalui penyebaran kuesioner online menggunakan platform Google Forms. Metode ini diadopsi karena efisiensinya dalam menjangkau responden dan kemudahannya dalam pengelolaan data awal, sebuah praktik yang umum dalam studi-studi kontemporer mengenai persepsi pengguna teknologi.

Responden dalam penelitian ini adalah 50 mahasiswa dari semester 4 sampai semester 6 yang berasal dari Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Esa Unggul, Kampus Bekasi. *Purposive sampling* digunakan untuk memilih kelompok responden ini karena mereka memiliki pemahaman dasar tentang teknologi informasi yang relevan dan tingkat penggunaan SIAKAD yang cukup tinggi. Asumsi ini sejalan dengan fokus pada subjek dengan latar belakang teknis seperti mahasiswa teknik informatika dalam penelitian Nurdin dan Rahman (2023), yang memungkinkan perolehan perspektif yang lebih mendalam terkait isu keamanan siber, meskipun kesadaran itu sendiri tetap menjadi variabel yang diukur.

Instrumen Penelitian, Pengumpulan, dan Analisis Data

Alat pengumpulan data primer dalam riset ini berupa angket digital yang memuat 10 butir pertanyaan dengan format yang telah ditentukan. Pertanyaan-pertanyaan ini dirancang untuk menggali dua variabel utama: pertama, tingkat kesadaran keamanan siber mahasiswa, yang mencakup aspek pemahaman akan ancaman siber, praktik aman seperti manajemen kata sandi, dan respons terhadap potensi insiden keamanan; kedua, tingkat kepercayaan mereka terhadap SIAKAD, yang meliputi aspek keamanan data pribadi, integritas informasi akademik, dan keandalan fungsionalitas sistem. Penyusunan item pertanyaan ini merujuk pada berbagai studi mengenai elemen-elemen kesadaran keamanan siber (Adzkia et al., 2024; Khando et al., 2021) dan faktor-faktor yang membentuk kepercayaan pengguna terhadap sistem informasi (Febriana & Indrarini, 2024). Penyebaran kuesioner dilakukan melalui platform media sosial WhatsApp kepada grup-grup mahasiswa yang relevan dalam periode waktu yang telah ditentukan.

Setelah data dari 50 responden terkumpul, langkah selanjutnya adalah data diolah secara manual. Pengolahan data awal ini melibatkan tabulasi jawaban dan, jika relevan, pemberian skor untuk item-item tertentu. Data akan dibagi menjadi empat kategori untuk pertanyaan yang berkaitan dengan penilaian atau persepsi. Kategori-kategori ini adalah sangat penting, cukup penting, kurang penting, dan tidak penting. Alternatif lainnya adalah menggunakan skala Likert untuk mengukur sikap dan persepsi responden. Dilanjutkan dengan menganalisis data yang dapat membantu menjawab pertanyaan penelitian. Perhitungan distribusi frekuensi dan persentase serta statistik deskriptif lainnya akan menjadi fokus analisis data. Pada akhirnya, analisis data ini akan dilakukan untuk memahami pola dan tren yang muncul dalam respons siswa. Tujuan akhir dari analisis ini adalah untuk memberikan gambaran tentang bagaimana kesadaran siswa tentang keamanan internet mempengaruhi kepercayaan mereka dalam menggunakan sistem pendidikan tersebut. Dengan demikian, analisis ini akan dapat memberikan kontribusi serupa dengan penelitian yang menemukan peran siswa dalam meningkatkan kesadaran tentang keamanan internet di lingkungan kampus (Jasmine et al., 2025).

HASIL DAN PEMBAHASAN

Menentukan Responden dan Perancangan Kuesioner

Data pribadi ini digunakan untuk kepentingan demografis responden dalam analisis dan tidak akan dipublikasikan secara individu.

Penentuan Responden

Penelitian ini menggunakan metode *purposive sampling*, yaitu pemilihan sampel secara sengaja berdasarkan kriteria tertentu. Responden ditargetkan adalah mahasiswa semester 4 hingga semester 6 dari Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Esa Unggul Kampus Bekasi. Mereka dianggap memiliki tingkat Studi Pengaruh Kesadaran ...

pemahaman yang relevan mengenai teknologi informasi serta intensitas penggunaan SIAKAD yang tinggi, sehingga sesuai untuk menjawab variabel penelitian.

Perancangan Kuesioner

Kuesioner penelitian ini dirancang dalam format digital menggunakan Google Form dan terdiri dari 26 pernyataan. Instrumen ini menggunakan skala Likert 4 poin. Untuk pernyataan favorable, pilihan jawaban diberikan dari 1 (Sangat Tidak Sesuai) hingga 4 (Sangat Sesuai). Sebaliknya, untuk pernyataan unfavorable, urutan penilaiannya dibalik, di mana 1 berarti Sangat Sesuai dan 4 berarti Sangat Tidak Sesuai. Ke-26 pernyataan tersebut dibagi menjadi dua indikator utama, yaitu Kesadaran Keamanan Siber (Cybersecurity Awareness) dan Kepercayaan terhadap SIAKAD (User Trust).

Tabel 1. Butir Pernyataan Kuesioner Mengenai Kesadaran Keamanan Siber dan Kepercayaan Pengguna terhadap SIAKAD

No.	Statement	Type
1	Saya merasa yakin bahwa SIAKAD memiliki sistem keamanan data pribadi yang baik.	Favorable
2	Saya selalu menggunakan kata sandi yang kuat dan unik untuk mengakses SIAKAD.	Favorable
3	Saya merasa tidak perlu menerapkan tindakan keamanan saat mengakses SIAKAD.	Unfavorable
4	Saya tidak yakin bahwa kampus peduli terhadap keamanan data mahasiswa dalam SIAKAD.	Unfavorable
5	Saya tidak pernah memperbarui kata sandi akun SIAKAD karena merasa tidak penting.	Unfavorable
6	Saya memahami pentingnya menghindari akses ke SIAKAD melalui jaringan publik tanpa VPN.	Favorable
7	Saya yakin bahwa pihak kampus telah menerapkan sistem cyber security yang memadai pada SIAKAD.	Favorable
8	Saya merasa tidak perlu memahami risiko keamanan saat menggunakan aplikasi kampus.	Unfavorable
9	Saya memiliki kesadaran untuk tidak membagikan informasi login SIAKAD kepada siapapun.	Favorable
10	Saya rutin mengganti password akun SIAKAD untuk meningkatkan keamanan.	Favorable
11	Saya memahami risiko serangan siber seperti phishing saat menggunakan layanan digital seperti SIAKAD.	Favorable
12	Saya sering menggunakan kata sandi yang sama untuk semua akun, termasuk SIAKAD.	Unfavorable
13	Saya merasa tidak ada ancaman nyata terhadap keamanan data akademik di SIAKAD.	Unfavorable
14	Saya jarang memperhatikan apakah koneksi jaringan saya aman saat login ke SIAKAD.	Unfavorable
15	Saya percaya bahwa edukasi tentang keamanan digital tidak berdampak pada penggunaan SIAKAD.	Unfavorable
16	Saya mempercayai bahwa data akademik saya tersimpan dengan aman dalam sistem SIAKAD.	Favorable
17	Saya merasa SIAKAD sangat responsif terhadap isu-isu keamanan digital.	Favorable
18	Saya tahu bagaimana cara melaporkan insiden keamanan data di SIAKAD.	Favorable
19	Saya merasa tidak perlu ikut serta dalam pelatihan keamanan siber dari pihak kampus.	Unfavorable
20	Saya cenderung mengabaikan peringatan keamanan dari sistem ketika mengakses SIAKAD.	Unfavorable
21	Saya tidak mengetahui bagaimana cara menangani jika terjadi kebocoran data di SIAKAD.	Unfavorable
22	Saya tidak peduli apakah data saya disalahgunakan oleh pihak yang tidak bertanggung jawab.	Unfavorable
23	Saya mendukung adanya pelatihan atau sosialisasi tentang keamanan siber di lingkungan kampus.	Favorable

Tabel 2. Butir Pernyataan Kuesioner Mengenai Kesadaran Keamanan Siber dan Kepercayaan Pengguna terhadap SIAKAD

No.	Statement	Type
24	Saya merasa lebih nyaman menggunakan SIAKAD setelah mengetahui langkah-langkah keamanannya.	Favorable
25	Saya yakin kesadaran keamanan siber penting dalam menjaga integritas data akademik.	Favorable
26	Saya lebih fokus pada kemudahan akses daripada keamanan ketika menggunakan SIAKAD.	Unfavorable

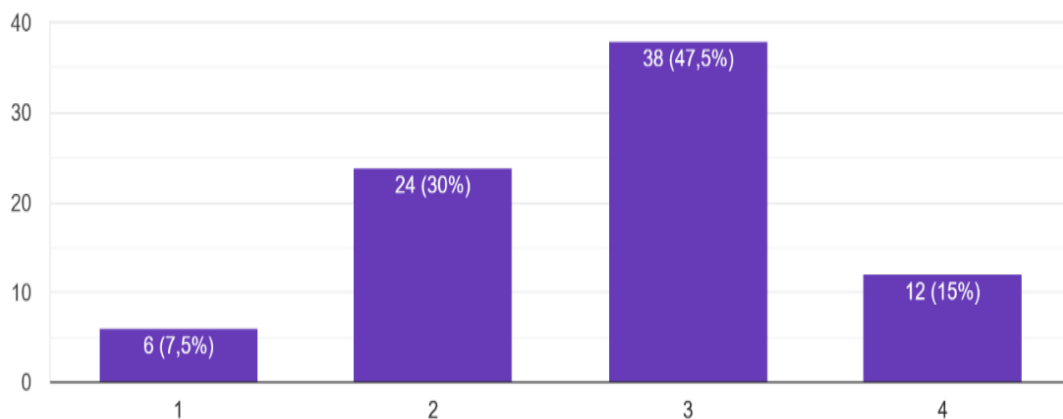
Penyebaran Kuesioner

Penyebaran kuesioner dilakukan secara efektif dengan mendistribusikan kuesioner kepada 80 responden yang terdiri dari mahasiswa Universitas Esa Unggul. Melalui penggunaan platform online, kuesioner disebarkan melalui media WhatsApp menggunakan Google Form, sehingga memungkinkan pengumpulan data secara praktis, efisien, dan menjangkau responden secara luas tanpa keterbatasan ruang dan waktu. Pendekatan ini dinilai tepat mengingat mayoritas mahasiswa sudah terbiasa dengan penggunaan perangkat digital dan media sosial dalam aktivitas sehari-hari.

Analisis Data

Saya merasa yakin bahwa SIAKAD memiliki sistem keamanan data pribadi yang baik.

80 jawaban

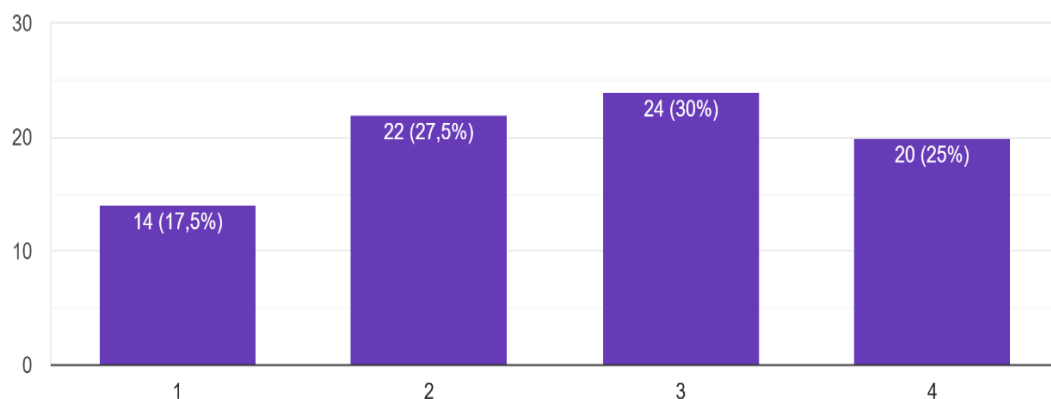


Gambar 1. Tingkat Keyakinan Mahasiswa terhadap Keamanan Data Pribadi di SIAKAD

Mayoritas responden menunjukkan tingkat kepercayaan yang tinggi terhadap sistem keamanan data di SIAKAD. Hal ini mencerminkan bahwa sistem dianggap cukup andal dalam menjaga privasi dan informasi pribadi mahasiswa.

Saya selalu menggunakan kata sandi yang kuat dan unik untuk mengakses SIAKAD.

80 jawaban

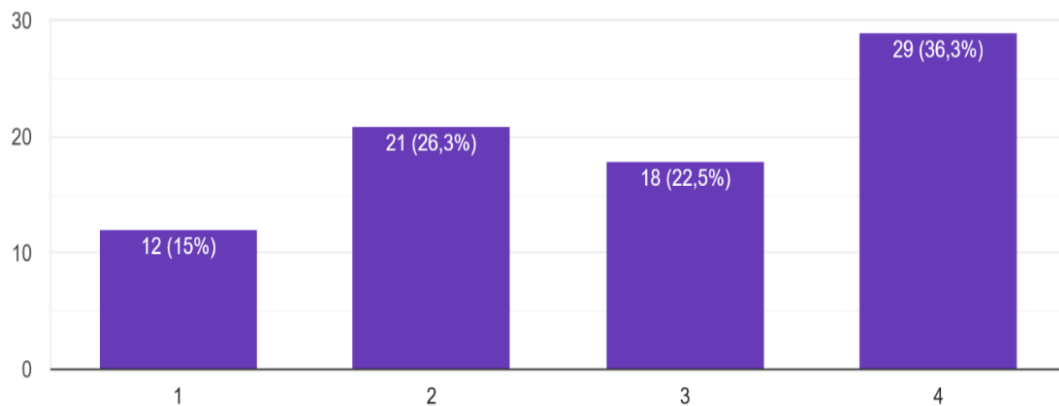


Gambar 2. Penggunaan Kata Sandi yang Kuat dan Unik untuk Akses SIAKAD

Sebagian besar mahasiswa menyatakan telah menggunakan kata sandi yang kuat dan tidak umum. Hal ini menunjukkan kesadaran keamanan pada aspek autentikasi cukup tinggi, meskipun sebagian kecil mungkin masih menggunakan pola kata sandi yang lemah.

Saya merasa tidak perlu menerapkan tindakan keamanan saat mengakses SIAKAD.

80 jawaban

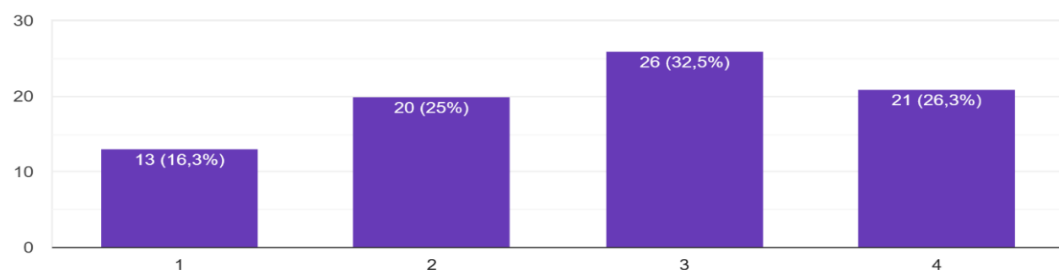


Gambar 3. Persepsi Mahasiswa terhadap Pentingnya Tindakan Keamanan saat Mengakses SIAKAD

Masih terdapat sejumlah mahasiswa yang merasa tindakan keamanan tambahan tidak perlu. Ini menandakan adanya celah kesadaran terkait pentingnya praktik keamanan dasar dalam penggunaan sistem informasi akademik.

Saya tidak yakin bahwa kampus peduli terhadap keamanan data mahasiswa dalam SIAKAD.

80 jawaban

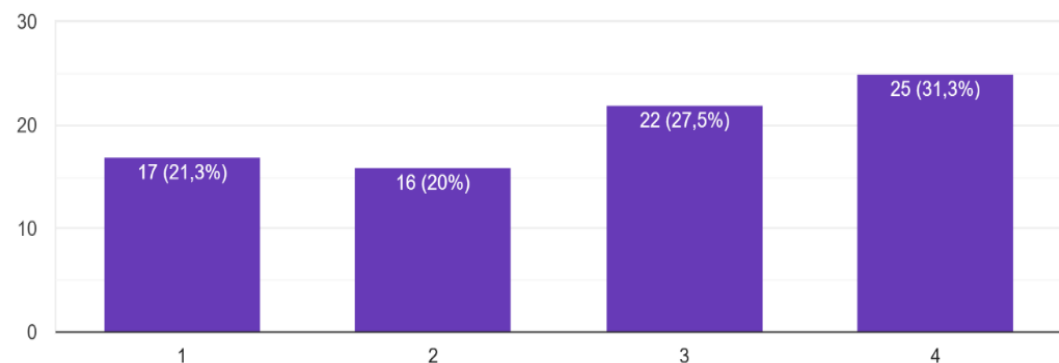


Gambar 4. Keyakinan Mahasiswa terhadap Kepedulian Kampus terhadap Keamanan Data di SIAKAD

Sebagian responden menunjukkan keraguan terhadap komitmen kampus dalam menjaga keamanan data. Keraguan ini bisa menjadi penghambat dalam menumbuhkan kepercayaan penuh terhadap SIAKAD.

Saya tidak pernah memperbarui kata sandi akun SIAKAD karena merasa tidak penting.

80 jawaban

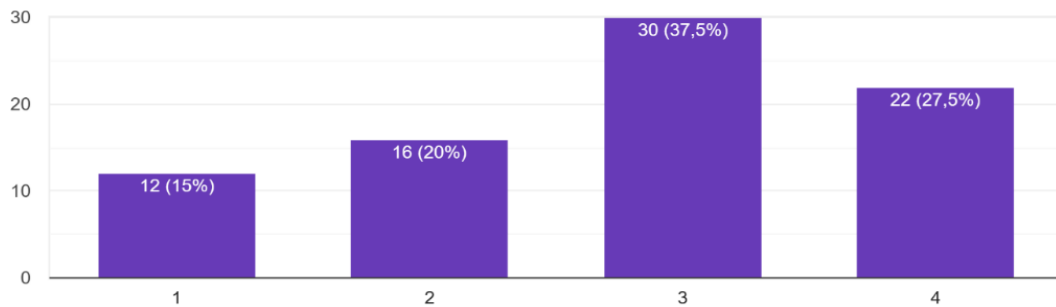


Gambar 5. Kebiasaan Pembaruan Kata Sandi Akun SIAKAD oleh Mahasiswa

Masih banyak mahasiswa yang tidak rutin memperbarui kata sandi, menandakan bahwa kebiasaan keamanan digital seperti penggantian password belum menjadi budaya yang kuat di kalangan mahasiswa.

Saya memahami pentingnya menghindari akses ke SIAKAD melalui jaringan publik tanpa VPN.

80 jawaban

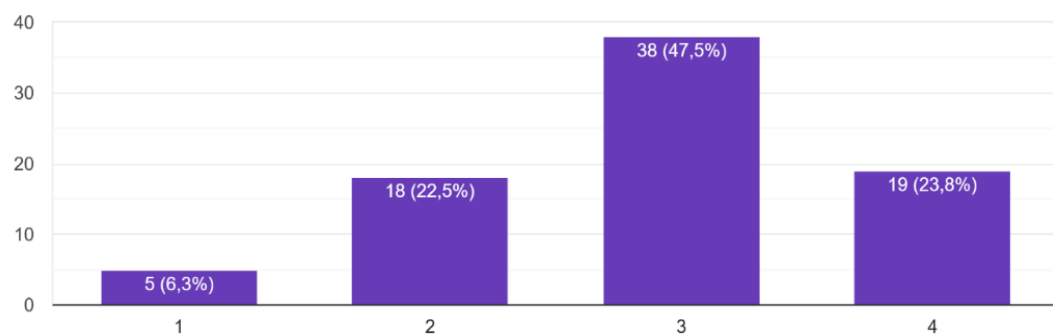


Gambar 6. Pemahaman Mahasiswa tentang Risiko Mengakses SIAKAD Melalui Jaringan Publik Tanpa VPN

Sebagian besar responden menunjukkan pemahaman yang baik terhadap risiko menggunakan jaringan publik tanpa perlindungan. Ini menunjukkan efektivitas penyuluhan atau pengetahuan umum mengenai keamanan jaringan.

Saya yakin bahwa pihak kampus telah menerapkan sistem cyber security yang memadai pada SIAKAD.

80 jawaban

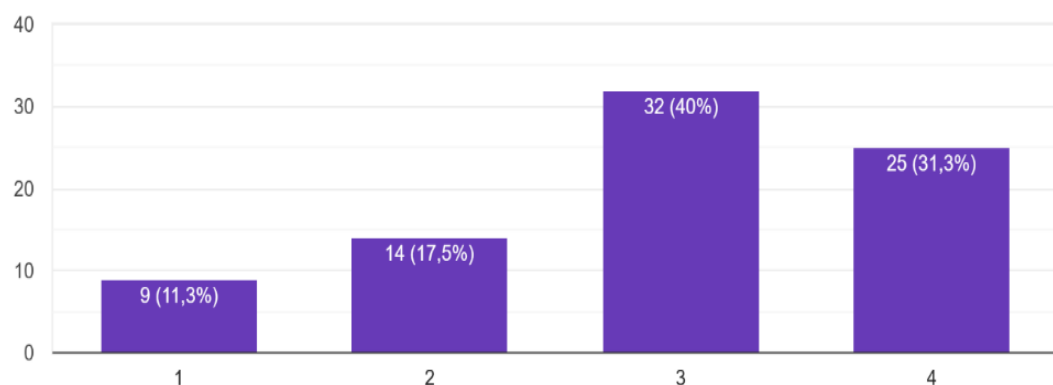


Gambar 7. Kepercayaan terhadap Implementasi Sistem Cyber Security oleh Kampus pada SIAKAD

Mahasiswa umumnya menaruh kepercayaan terhadap sistem keamanan yang telah diterapkan kampus. Ini merupakan modal penting dalam membangun relasi yang baik antara pengguna dan institusi penyedia layanan.

Saya merasa tidak perlu memahami risiko keamanan saat menggunakan aplikasi kampus.

80 jawaban

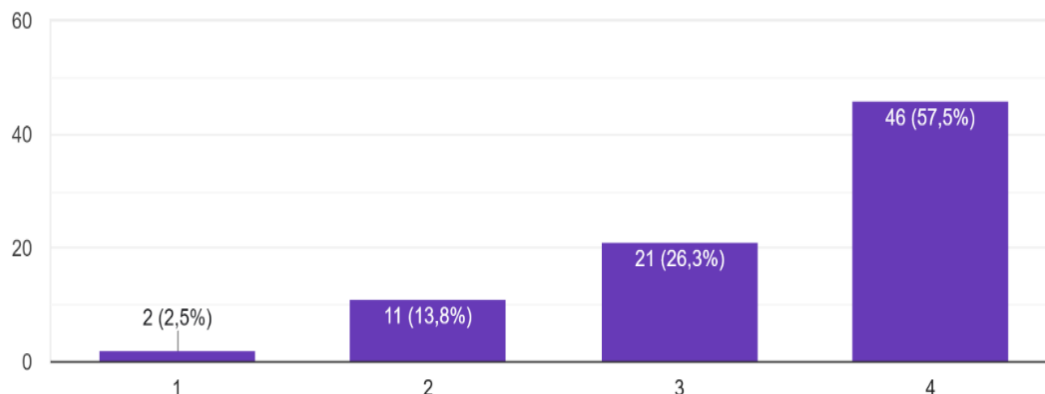


Gambar 8. Persepsi Mahasiswa terhadap Pentingnya Memahami Risiko Keamanan Aplikasi Kampus

Beberapa responden masih menunjukkan sikap apatis terhadap pentingnya pemahaman risiko. Hal ini mencerminkan perlunya peningkatan literasi keamanan siber secara menyeluruh.

Saya memiliki kesadaran untuk tidak membagikan informasi login SIAKAD kepada siapapun.

80 jawaban

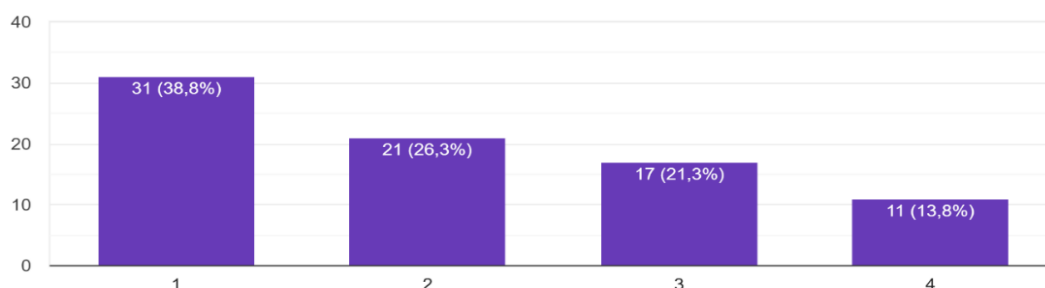


Gambar 9. Kesadaran Mahasiswa untuk Tidak Membagikan Informasi Login SIAKAD

Mayoritas mahasiswa sadar akan pentingnya menjaga kerahasiaan informasi login, mencerminkan kesadaran dasar terhadap prinsip keamanan informasi.

Saya rutin mengganti password akun SIAKAD untuk meningkatkan keamanan.

80 jawaban

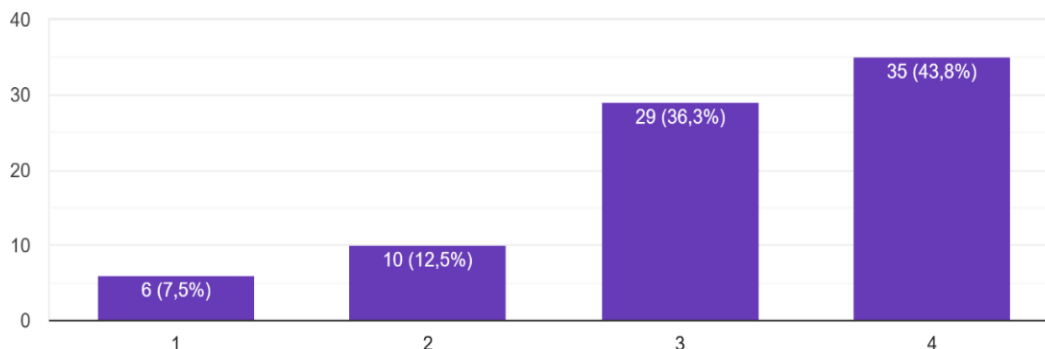


Gambar 10. Kebiasaan Mahasiswa dalam Mengganti Kata Sandi Akun SIAKAD secara Berkala

Kebiasaan mengganti password belum sepenuhnya dilakukan oleh semua responden. Hal ini memperlihatkan bahwa meskipun ada kesadaran, belum semua mahasiswa menerapkan praktik keamanan secara konsisten.

Saya memahami risiko serangan siber seperti phishing saat menggunakan layanan digital seperti SIAKAD.

80 jawaban

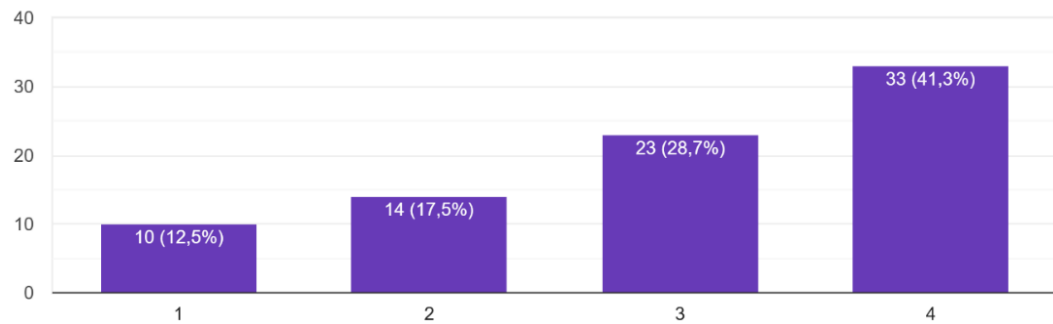


Gambar 11. Pemahaman Mahasiswa terhadap Risiko Serangan Siber Seperti Phishing di SIAKAD

Sebagian besar responden telah memahami ancaman serangan seperti phishing, yang menunjukkan tingkat kesadaran terhadap bentuk-bentuk serangan digital cukup baik.

Saya sering menggunakan kata sandi yang sama untuk semua akun, termasuk SIAKAD.

80 jawaban

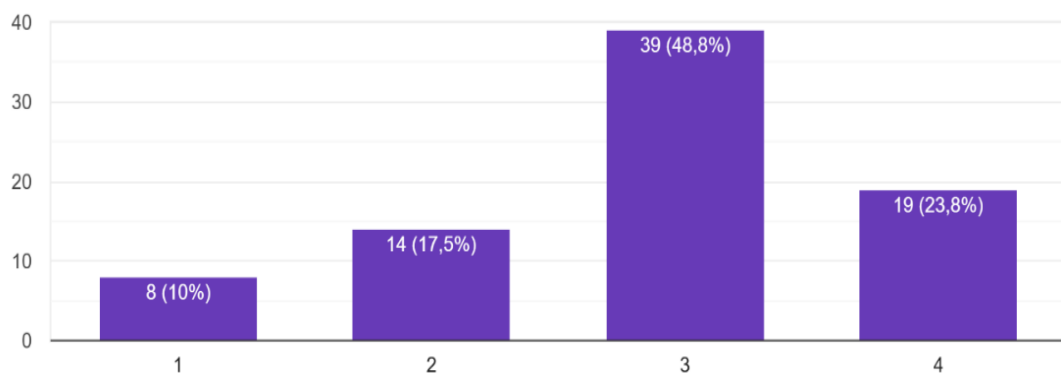


Gambar 12. Penggunaan Kata Sandi yang Sama pada Berbagai Akun Termasuk SIAKAD

Masih banyak responden yang menggunakan kata sandi sama untuk beberapa akun. Praktik ini meningkatkan risiko keamanan dan menunjukkan bahwa edukasi tentang segmentasi password perlu diperkuat.

Saya merasa tidak ada ancaman nyata terhadap keamanan data akademik di SIAKAD.

80 jawaban

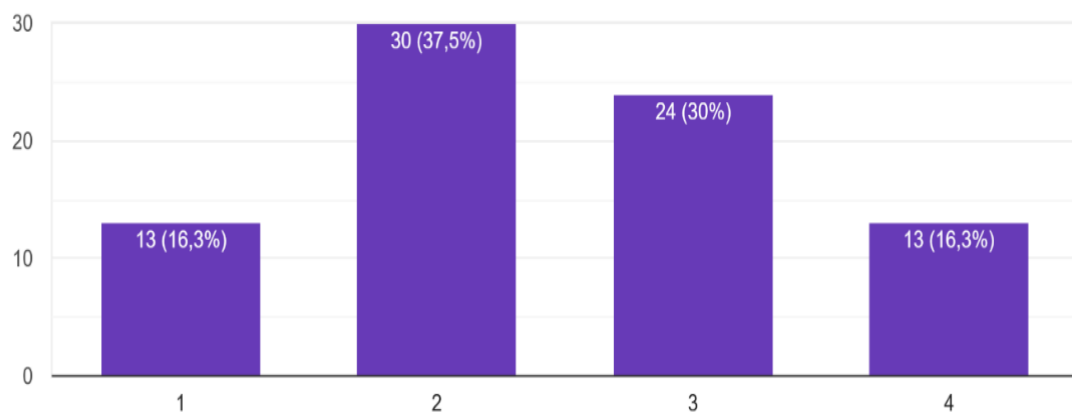


Gambar 13. Persepsi Mahasiswa terhadap Ancaman Keamanan Data Akademik di SIAKAD

Sebagian mahasiswa tidak melihat adanya ancaman nyata, yang menandakan bahwa persepsi risiko terhadap ancaman siber masih rendah di kalangan tertentu.

Saya jarang memperhatikan apakah koneksi jaringan saya aman saat login ke SIAKAD.

80 jawaban

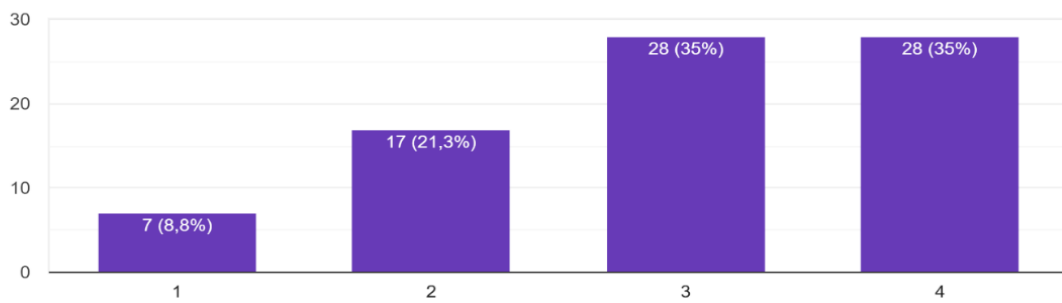


Gambar 14. Kebiasaan Mahasiswa dalam Memperhatikan Keamanan Jaringan saat Login ke SIAKAD

Banyak mahasiswa tidak memeriksa keamanan koneksi saat mengakses SIAKAD, yang menunjukkan kurangnya perhatian terhadap aspek perlindungan jaringan pribadi.

Saya percaya bahwa edukasi tentang keamanan digital tidak berdampak pada penggunaan SIAKAD.

80 jawaban

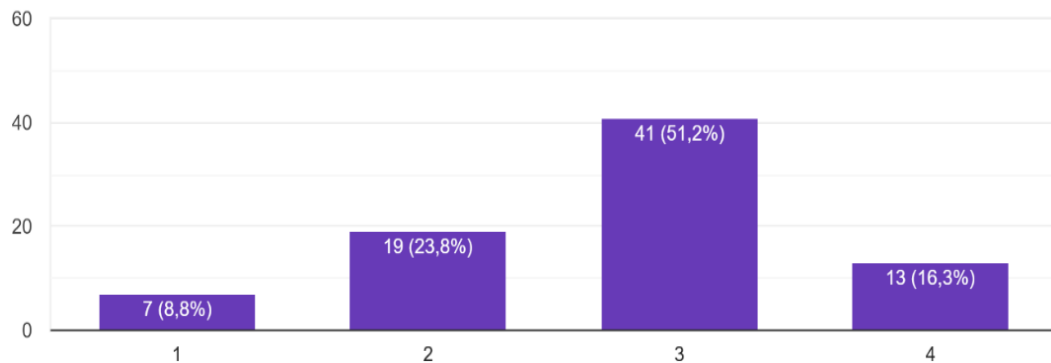


Gambar 15. Pandangan Mahasiswa tentang Dampak Edukasi Keamanan Digital terhadap Penggunaan SIAKAD

Sebagian responden merasa edukasi tidak berpengaruh terhadap kebiasaan mereka dalam menggunakan SIAKAD. Hal ini menjadi indikator bahwa pendekatan edukasi yang dilakukan saat ini perlu ditinjau ulang agar lebih efektif.

Saya mempercayai bahwa data akademik saya tersimpan dengan aman dalam sistem SIAKAD.

80 jawaban

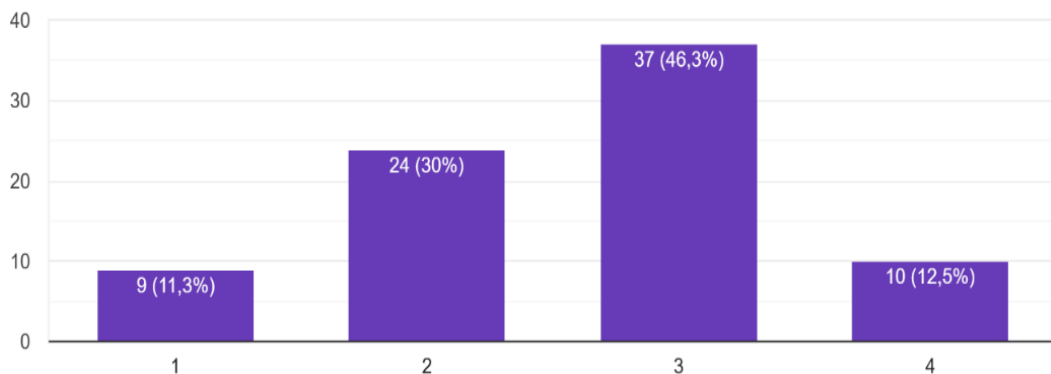


Gambar 16. Keyakinan Mahasiswa terhadap Keamanan Penyimpanan Data Akademik di SIAKAD

Sebagian besar mahasiswa menunjukkan tingkat kepercayaan yang tinggi terhadap sistem penyimpanan data SIAKAD. Ini memperlihatkan bahwa persepsi terhadap keamanan sistem masih positif.

Saya merasa SIAKAD sangat responsif terhadap isu-isu keamanan digital.

80 jawaban

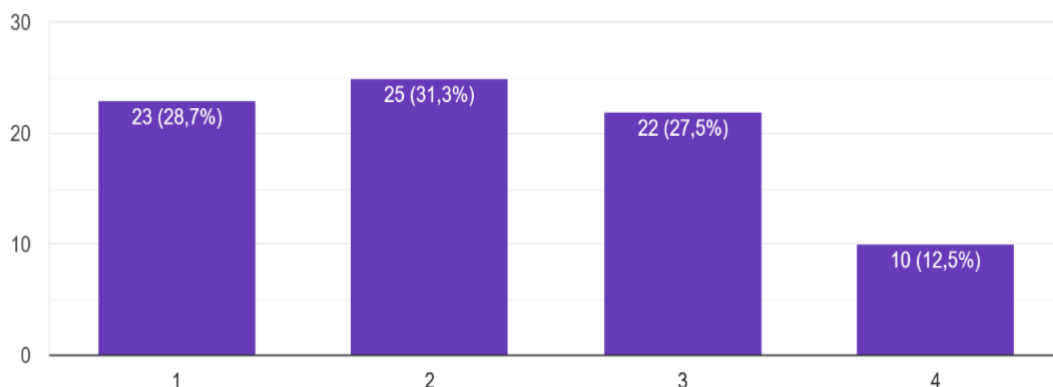


Gambar 17. Responsivitas SIAKAD terhadap Isu-Isu Keamanan Digital Menurut Mahasiswa

Mahasiswa menilai SIAKAD cukup tanggap dalam menangani masalah keamanan, yang menunjukkan bahwa sistem telah memberikan feedback atau penanganan yang sesuai saat terjadi potensi ancaman.

Saya tahu bagaimana cara melaporkan insiden keamanan data di SIAKAD.

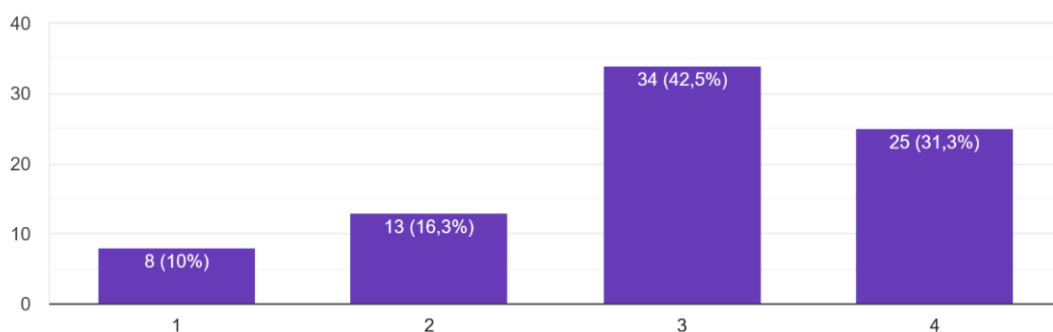
80 jawaban

**Gambar 18.** Pengetahuan Mahasiswa tentang Cara Melaporkan Insiden Keamanan Data di SIAKAD

Sebagian responden mengetahui prosedur pelaporan insiden, namun belum menyeluruh. Ini menandakan perlunya penyebarluasan informasi mengenai SOP penanganan insiden.

Saya merasa tidak perlu ikut serta dalam pelatihan keamanan siber dari pihak kampus.

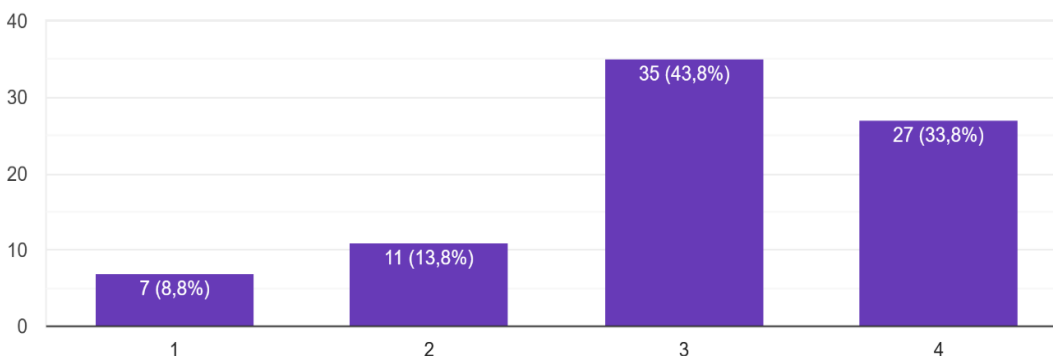
80 jawaban

**Gambar 19.** Partisipasi Mahasiswa dalam Pelatihan Keamanan Siber oleh Pihak Kampus

Sebagian mahasiswa merasa tidak membutuhkan pelatihan keamanan, yang menandakan bahwa motivasi dan minat terhadap peningkatan kapasitas keamanan pribadi masih rendah di sebagian kalangan.

Saya cenderung mengabaikan peringatan keamanan dari sistem ketika mengakses SIAKAD.

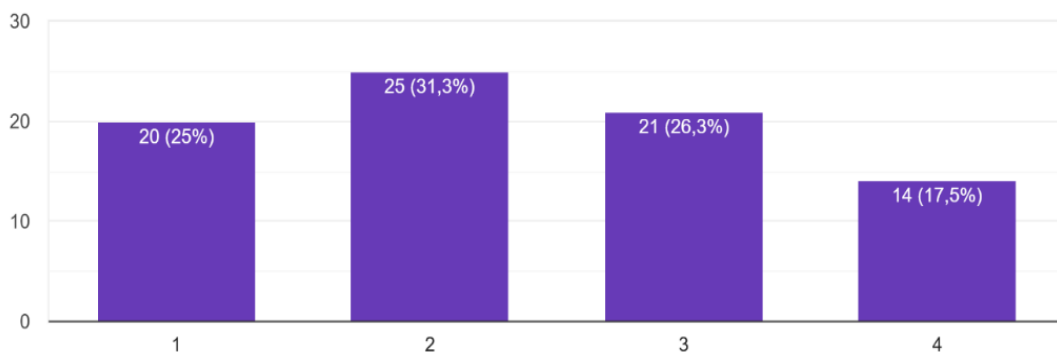
80 jawaban

**Gambar 20.** Sikap Mahasiswa terhadap Peringatan Keamanan saat Mengakses SIAKAD

Terdapat kecenderungan untuk mengabaikan peringatan sistem, yang menunjukkan bahwa sistem perlu memperkuat cara penyampaian informasi agar tidak diabaikan..

Saya tidak mengetahui bagaimana cara menangani jika terjadi kebocoran data di SIAKAD.

80 jawaban

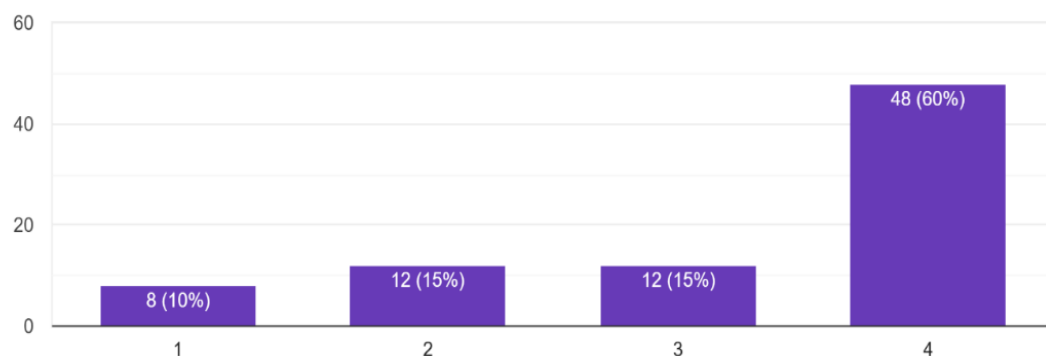


Gambar 21. Pengetahuan Mahasiswa dalam Menangani Insiden Kebocoran Data di SIAKAD

Banyak mahasiswa tidak tahu tindakan yang harus dilakukan saat terjadi kebocoran data. Hal ini menunjukkan adanya kekurangan dalam penyampaian informasi prosedural terkait respons insiden.

Saya tidak peduli apakah data saya disalahgunakan oleh pihak yang tidak bertanggung jawab.

80 jawaban

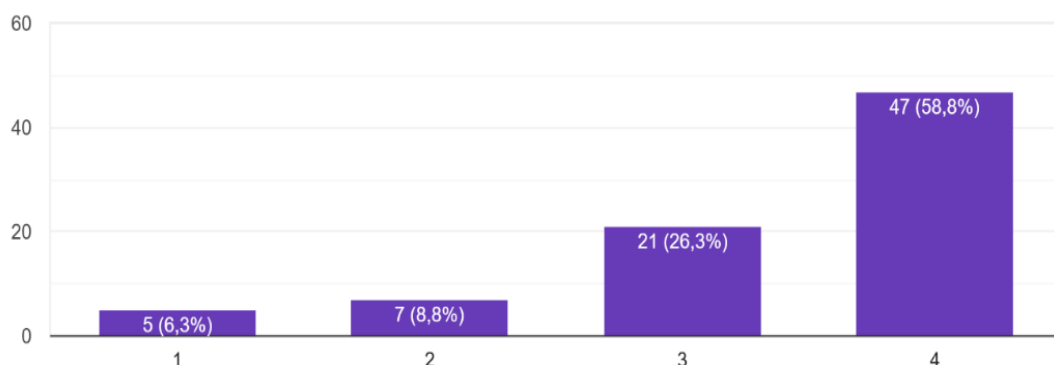


Gambar 22. Kepedulian Mahasiswa terhadap Penyalahgunaan Data oleh Pihak Tidak Bertanggung Jawab

Adanya responden yang tidak peduli terhadap penyalahgunaan data menunjukkan tingkat literasi keamanan data pribadi masih kurang di beberapa kalangan.

Saya mendukung adanya pelatihan atau sosialisasi tentang keamanan siber di lingkungan kampus.

80 jawaban

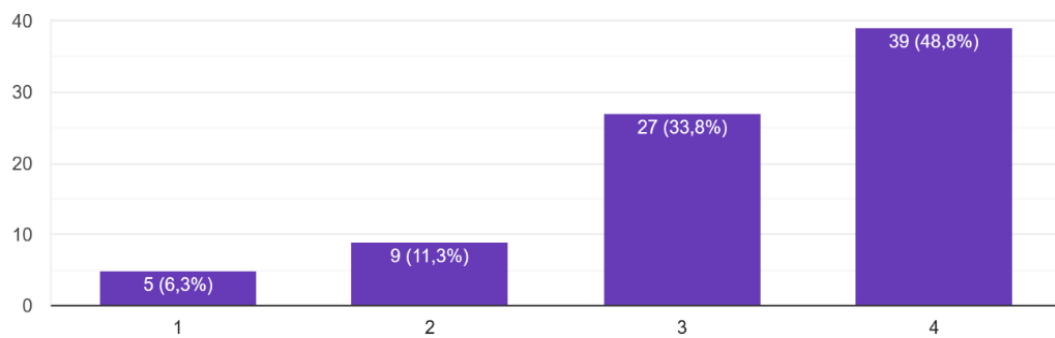


Gambar 23. Dukungan Mahasiswa terhadap Program Pelatihan atau Sosialisasi Keamanan Siber di Kampus

Mayoritas mahasiswa menunjukkan dukungan terhadap inisiatif kampus dalam memberikan pelatihan keamanan, memberikan peluang besar untuk meningkatkan kesadaran kolektif.

Saya merasa lebih nyaman menggunakan SIAKAD setelah mengetahui langkah-langkah keamanannya.

80 jawaban

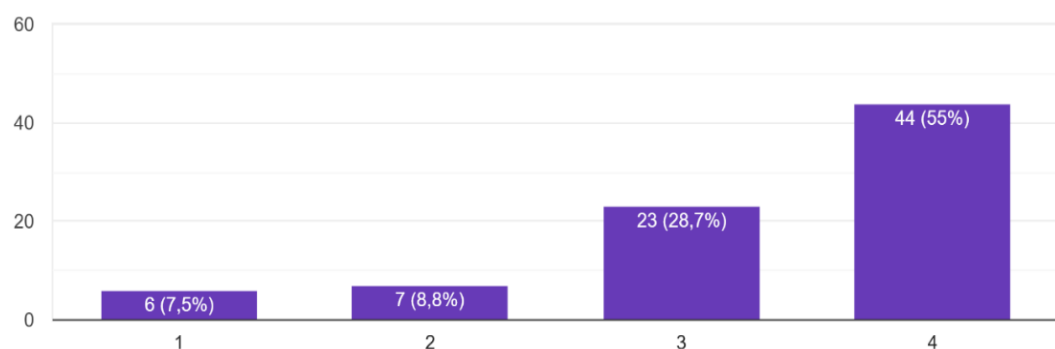


Gambar 24. Kenyamanan Mahasiswa Menggunakan SIAKAD setelah Mengetahui Fitur Keamanannya

Mahasiswa merasa lebih nyaman setelah memahami aspek keamanan sistem, yang menegaskan bahwa transparansi keamanan sistem mampu meningkatkan kenyamanan dan kepercayaan pengguna.

Saya yakin kesadaran keamanan siber penting dalam menjaga integritas data akademik.

80 jawaban

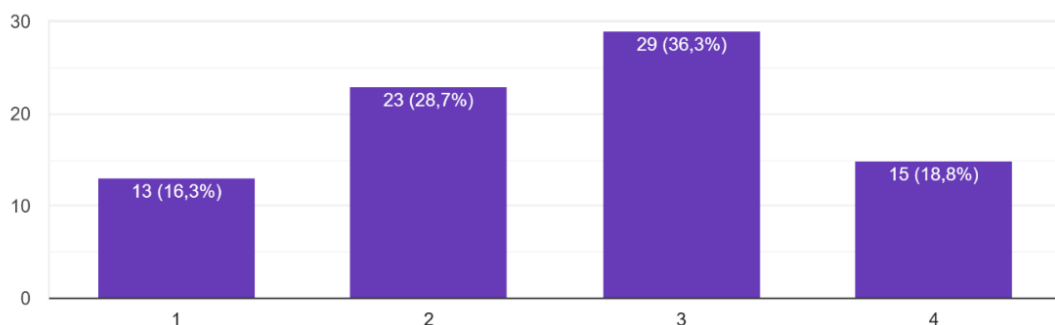


Gambar 25. Pandangan Mahasiswa tentang Pentingnya Kesadaran Keamanan Siber dalam Menjaga Integritas Data Akademik

Sebagian besar responden menyadari pentingnya kesadaran keamanan siber, menjadi sinyal positif bahwa mahasiswa memiliki pemahaman akan dampak nyata dari keamanan digital terhadap data mereka.

Saya lebih fokus pada kemudahan akses daripada keamanan ketika menggunakan SIAKAD.

80 jawaban



Gambar 26. Preferensi Mahasiswa terhadap Kemudahan Akses Dibandingkan Keamanan saat Menggunakan SIAKAD

Sebagian mahasiswa lebih mementingkan kemudahan akses daripada aspek keamanan. Ini mengindikasikan bahwa ada trade-off yang dirasakan antara user experience dan proteksi data, yang harus diatasi melalui edukasi dan desain sistem yang seimbang.

KESIMPULAN DAN SARAN

Simpulan

Berdasarkan analisis deskriptif kuantitatif terhadap 80 responden mahasiswa Fakultas Ilmu Komputer Universitas Esa Unggul, penelitian ini menyimpulkan bahwa ada hubungan erat antara kesadaran keamanan siber dan kepercayaan pengguna terhadap SIAKAD. Secara umum, mahasiswa menunjukkan tingkat kepercayaan yang cukup tinggi terhadap kapabilitas teknis SIAKAD, meyakini bahwa sistem tersebut memiliki keamanan data yang baik. Kepercayaan ini meningkat seiring dengan pengetahuan mahasiswa tentang langkah-langkah keamanan yang diterapkan. Meskipun demikian, kepercayaan ini tidaklah mutlak, karena sebagian responden masih ragu terhadap kepedulian kampus dalam menjaga keamanan data, yang berpotensi mengikis kepercayaan secara keseluruhan.

Penelitian ini juga menyoroti adanya kesenjangan antara pengetahuan dan praktik keamanan siber di kalangan mahasiswa. Meskipun mayoritas responden memahami konsep dasar keamanan seperti risiko phishing dan pentingnya tidak membagikan informasi login, pengetahuan ini tidak selalu diterjemahkan ke dalam praktik sehari-hari. Banyak mahasiswa yang tidak rutin mengganti kata sandi atau menggunakan kata sandi yang sama untuk berbagai akun. Selain itu, ditemukan sikap apatis dan persepsi risiko yang rendah di kalangan mahasiswa, yang cenderung mengabaikan peringatan keamanan dan lebih memprioritaskan kemudahan akses daripada keamanan.

Celah terbesar dalam kesadaran keamanan siber mahasiswa terletak pada kurangnya pengetahuan prosedural. Banyak responden tidak tahu cara melaporkan insiden keamanan data atau tindakan yang harus dilakukan jika terjadi kebocoran data. Hal ini menunjukkan bahwa, meskipun kepercayaan terhadap sistem itu sendiri cukup tinggi, ancaman terbesar justru berasal dari inkonsistensi perilaku aman dari pengguna, yang didorong oleh sikap apatis dan kurangnya pengetahuan prosedural. Oleh karena itu, untuk membangun kepercayaan yang kokoh, edukasi yang terarah dan berkelanjutan untuk meningkatkan kesadaran dan praktik keamanan siber di kalangan mahasiswa sangat vital.

Saran

Berdasarkan temuan dan kesimpulan penelitian, disarankan agar pihak universitas, khususnya unit Teknologi Informasi dan Kemahasiswaan, mengembangkan program peningkatan kesadaran keamanan siber yang terstruktur dan berkelanjutan. Program ini dapat mencakup pelatihan rutin, sosialisasi, dan simulasi penanganan insiden keamanan data yang melibatkan partisipasi aktif mahasiswa. Selain itu, integrasi materi literasi keamanan digital ke dalam kurikulum yang relevan juga dapat menjadi langkah preventif jangka panjang untuk membentuk budaya sadar keamanan di lingkungan akademik.

Selanjutnya, mekanisme pelaporan insiden keamanan pada sistem SIAKAD perlu diperkuat, baik dari sisi kemudahan akses maupun kejelasan prosedurnya. Memudahkan mahasiswa untuk melaporkan potensi masalah dapat mempercepat respons dan membangun rasa aman. Perbaikan ini akan melengkapi upaya edukasi dengan menyediakan jalur komunikasi yang efektif dan tepercaya bagi pengguna.

Untuk pengembangan teori dan penelitian selanjutnya, studi ini membuka peluang untuk eksplorasi lebih dalam menggunakan metode campuran (mixed methods). Penelitian lanjutan dapat melibatkan responden dari berbagai program studi atau lintas universitas untuk memperluas generalisasi hasil. Dimensi variabel lain, seperti literasi digital, kekhawatiran privasi, dan niat perilaku, juga dapat ditambahkan untuk memperkaya pemahaman faktor-faktor yang mempengaruhi kepercayaan pengguna terhadap sistem informasi akademik. Selain itu, penelitian longitudinal dapat dilakukan untuk mengamati dampak intervensi edukasi keamanan siber dari waktu ke waktu dan mengukur perubahan kepercayaan pengguna secara lebih akurat.

REFERENCE

- Soesanto, E., Putri, S. C. T., Aulia, A. A., Wicaksana, F. Y., & Thalitha, R. F. (2023). Sistem pengamanan file dan cyber security pada pengamanan objek vital PT PDAM (Perusahaan Daerah Air Minum). *Cross-border*, 6(2), 766–774. <https://doi.org/10.24198/responsive.v1i2.20673>
- Faliandy, M. Y., Lazuardi, M. Y., & Sutabri, T. (2023). Analisis kesadaran keamanan siber pada pengguna aplikasi E-Court di lingkungan pengadilan. *Jurnal Ilmiah Binary STMIK Bina Nusantara Jaya*, 5(2), 101–107. <https://doi.org/10.52303/jb.v5i2.106>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 1–22. <https://doi.org/10.1016/j.cose.2021.102267>
- Nurdin, H., & Rahman, A. (2023). Pengukuran tingkat kesadaran keamanan siber pada pengguna media sosial di lingkungan mahasiswa Teknik Informatika Universitas Widyatama. *Jurnal Darma Agung*, 31(3), 94–102. <http://dx.doi.org/10.46930/ojsuda.v31i3.3374>
- Jasmine, N., Nafilah, A., & Rahmadanti, R. (2025). Peran mahasiswa dalam meningkatkan kesadaran keamanan siber di lingkungan kampus. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen, dan Keuangan*, 1(2), 109–121. <http://dx.doi.org/10.63217/fibonacci.v1i2.76>
- Mahendra, A., Hatta, P., & Aristyagama, Y. (2024). Analisis tingkat kesadaran keamanan cyber di media sosial Instagram: Studi kasus pada siswa SMK Negeri 1 Banyudono. *BINA INSANI ICT Journal*, 11(1), 86–99. <http://dx.doi.org/10.51211/biict.v11i1.2963>
- Adzkia, M. K., Samudi, & Ningsih, S. R. (2024). Kesadaran keamanan siber pada kalangan mahasiswa Universitas di Kota Batam. *JATI (Jurnal Mahasiswa Teknologi Informasi)*, 14(2), 163–173. <https://doi.org/10.34010/jati.v14i2.12518>
- Febriana, V. C., & Indrarini, R. (2024). Pengaruh cyber crime dan cyber security terhadap tingkat kepercayaan nasabah bank syariah dalam menggunakan layanan M-Banking di wilayah Surabaya. *JEKoBi*, 7(3), 161–174. <https://doi.org/10.26740/jekobi.v7n3.p161-174>
- Y. W., Fitriana, Y. B., Esabella, S., Yuwono, D. T., & Surya, R. A. (2025). Optimasi cyber security keamanan e-government Kominfo Kab. Sumbawa 2024 menggunakan metode kuantitatif. *Digitech*, 4(2), 1206–1216. <https://doi.org/10.47709/digitech.v4i2.5383>