

SERTIFIKAT PENILAIAN KESADARAN
KEAMANAN SIBER

Dengan ini menyatakan bahwa

sdsaddsada

telah menyelesaikan penilaian kesadaran keamanan siber dengan skor

60.8%

dengan tingkat kesadaran keamanan siber

Sedang

pada tanggal 10 April 2025

Diterbitkan oleh Tim Penilai Kesadaran Keamanan Siber



HASIL PENILAIAN KESADARAN KEAMANAN SIBER

Kesadaran Teknis

62.8%

Kesadaran Sosial

58.8%

Skor Keseluruhan

60.8%

Tingkat Kesadaran Keamanan Siber: **Sedang**

Kesadaran Keamanan Siber Teknis

Terms and Conditions of Device / Application Installation	66.7%
Setting Controls and Updates	60.0%
Backup and Data Recovery	62.5%
Encryption and Protection	60.0%
Account and Authentication Security	65.0%

Kesadaran Keamanan Siber Sosial

Social Engineering Recognition	60.0%
Information Sharing Practices	55.0%
Online Privacy Management	62.5%
Online Transaction Security	50.0%
Cyber Incident Handling	66.7%

Hasil penilaian ini berdasarkan jawaban yang diberikan pada kuesioner kesadaran keamanan siber.

REKOMENDASI KEAMANAN SIBER YANG DIPERSONALISASI

Berdasarkan penilaian kesadaran keamanan siber yang telah dilakukan, berikut adalah rekomendasi yang disesuaikan dengan profil dan jawaban Anda:

Berdasarkan profil demografis dan respons kuesioner Anda, berikut ini adalah beberapa rekomendasi yang dapat Anda pertimbangkan:

1. **Edukasi Diri dan Pelatihan:** Memiliki latar belakang pendidikan sarjana, Anda harus memanfaatkan kemampuan Anda untuk belajar dan memahami konsep baru. Ikuti kursus online atau seminar tentang keamanan siber untuk lebih memahami ancaman yang ada dan cara melindungi diri Anda dari ancaman tersebut.
2. **Pengetahuan Teknis:** Anda perlu mengetahui cara kerja perangkat dan aplikasi yang Anda gunakan. Ini termasuk pemahaman tentang pengaturan privasi dan keamanan, serta pembaruan perangkat lunak dan operasi sistem.
3. **Gunakan Antivirus dan Firewall:** Gunakan perangkat lunak antivirus yang andal dan selalu aktifkan firewall pada komputer Anda. Ini akan memberi lapisan perlindungan tambahan terhadap serangan siber.
4. **Berhati-hati dengan Email dan Situs Web:** Banyak serangan siber dimulai dengan email phishing atau situs web yang meragukan. Selalu periksa alamat email pengirim dan URL situs web sebelum klik link atau download file.
5. **Buat Cadangan Data:** Buat cadangan data secara rutin untuk mencegah kehilangan data jika terjadi serangan siber. Anda dapat menggunakan layanan cloud atau perangkat penyimpanan eksternal.
6. **Perbarui Password:** Jangan gunakan password yang sama untuk semua akun. Buat password yang kuat yang mencakup kombinasi huruf, angka dan simbol.
7. **Tingkatkan Keamanan Jaringan:** Mengingat Anda berada di Jakarta, Indonesia, Anda mungkin berhadapan dengan risiko keamanan siber yang lebih tinggi. Pertimbangkan untuk menggunakan VPN saat mengakses internet dan selalu gunakan jaringan yang aman.
8. **Tetap Up-to-date:** Teknologi dan ancaman siber terus berkembang. Anda harus selalu up-to-date dengan tren dan ancaman keamanan siber terbaru. Ingatlah bahwa keamanan siber adalah tang