SERTIFIKAT PENILAIAN KESADARAN KEAMANAN SIBER

Dengan ini menyatakan bahwa

asdas

telah menyelesaikan penilaian kesadaran keamanan siber dengan skor

65.0%

dengan tingkat kesadaran keamanan siber

Sedang

pada tanggal 10 April 2025

Diterbitkan oleh Tim Penilai Kesadaran Keamanan Siber

SERTIFIKAT

HASIL PENILAIAN KESADARAN KEAMANAN SIBER

Kesadaran Teknis	Kesadaran Sosial	Skor Keseluruhan
68.1%	61.8%	65.0%

Tingkat Kesadaran Keamanan Siber: Sedang

Kesadaran Keamanan Siber Teknis

Terms and Conditions of Device / Application Installation	**66.7%**
Setting Controls and Updates	**65.0%**
Backup and Data Recovery	**68.8%**
Encryption and Protection	**65.0%**
Account and Authentication Security	**75.0%**

Kesadaran Keamanan Siber Sosial

Social Engineering Recognition	**65.0%**
Information Sharing Practices	**65.0%**
Online Privacy Management	**62.5%**
Online Transaction Security	**58.3%**
Cyber Incident Handling	**58.3%**

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, respons terhadap kuesioner, tingkat pendidikan, dan lokasi geografis, berikut adalah rekomendasi keamanan siber yang dapat diberikan kepada Bapak asdas: 1. Pelatihan Kesadaran Keamanan Siber: Mengingat latar belakang pendidikan master Anda dan respons kuesioner, disarankan untuk mengikuti pelatihan kesadaran keamanan siber yang lebih tinggi. Pelatihan ini akan membantu Anda memahami ancaman keamanan yang lebih kompleks dan cara melindungi diri dari serangan tersebut. 2. Autentikasi Dua Faktor: Gunakan autentikasi dua faktor (2FA) untuk semua akun online yang penting. Ini memberikan lapisan keamanan tambahan dan dapat mencegah penyerang mendapatkan akses meskipun mereka mengetahui kata sandi Anda. 3. Perbarui Sistem dan Aplikasi: Selalu perbarui sistem operasi dan aplikasi ke versi terbaru. Pembaruan ini seringkali mencakup perbaikan keamanan yang penting. 4. Penggunaan VPN: Mengingat Anda berada di Jakarta, Indonesia, penggunaan VPN disarankan untuk melindungi privasi Anda saat online. VPN akan mengenkripsi data Anda dan melindungi identitas Anda saat online. 5. Backup Data: Lakukan backup data secara berkala untuk mencegah kehilangan data jika terjadi serangan siber. 6. Penggunaan Antivirus: Gunakan solusi antivirus yang tepercaya dan selalu perbarui basis data virusnya. 7. Hati-hati dengan Email dan Lampirannya: Jangan buka email atau lampiran dari pengirim yang tidak dikenal. Ini bisa menjadi upaya phishing untuk mendapatkan informasi pribadi Anda. 8. Jangan Bagikan Informasi Pribadi: Jangan pernah memberikan informasi pribadi Anda kepada siapa pun melalui internet. Informasi ini bisa digunakan oleh penyerang untuk melancarkan serangan. 9. Gunakan Jaringan yang Aman: Hindari penggunaan jaringan WiFi publik yang tidak aman. J