SERTIFIKAT PENILAIAN KESADARAN KEAMANAN SIBER

Dengan ini menyatakan bahwa

sadadsa

telah menyelesaikan penilaian kesadaran keamanan siber dengan skor

65.2%

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
64.8%	65.5%	65.2%

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	**75.0%**
Account and Authentication Security	**60.0%**

Kesadaran Keamanan Siber Sosial

Social Engineering Recognition	**65.0%**
Information Sharing Practices	**75.0%**
Online Privacy Management	**62.5%**
Online Transaction Security	**66.7%**
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:

Rekomendasi Keamanan Siber: Berdasarkan profil demografis, respons kuesioner, tingkat pendidikan, dan lokasi geografis Anda, berikut adalah beberapa rekomendasi keamanan siber yang dipersonalisasi untuk Anda: 1. Pendidikan Keamanan Siber: Mengingat latar belakang pendidikan Anda adalah diploma, disarankan untuk mengambil kursus online atau seminar tentang keamanan siber. Ini akan membantu Anda memahami dasar-dasar keamanan siber, ancaman yang ada, dan bagaimana melindungi diri dari mereka. 2. Perangkat Lunak Keamanan: Pastikan Anda memiliki perangkat lunak anti-virus dan anti-malware yang terupdate pada semua perangkat Anda. Ini akan membantu melindungi Anda dari serangan siber. 3. Update Sistem: Sering-seringlah memperbarui sistem operasi dan aplikasi Anda. Pembaruan ini seringkali mencakup perbaikan keamanan penting. 4. Penggunaan Password: Gunakan password yang kuat dan berbeda untuk setiap akun Anda. Pertimbangkan untuk menggunakan manajer password untuk membantu Anda mengingat dan menyimpan password dengan aman. 5. Menghindari Phishing: Berhati-hatilah dengan email atau pesan yang mencurigakan, terutama yang meminta informasi pribadi Anda. Ini mungkin adalah upaya phishing. 6. Keamanan Jaringan: Jika Anda tinggal di Jakarta, risiko serangan siber mungkin lebih tinggi karena populasi dan aktivitas online yang tinggi. Pertimbangkan untuk menggunakan VPN saat mengakses internet, terutama di jaringan publik. 7. Backup Data: Buatlah backup data Anda secara reguler. Ini akan melindungi Anda jika perangkat Anda diserang oleh ransomware atau malware lainnya. 8. Privasi Online: Jadilah sadar akan informasi pribadi Anda yang diposting online. Hati-hati dengan apa yang Anda bagikan di media sosial dan situs lainnya. 9. Kesadaran Keamanan: Tetaplah waspada dan kritis terhadap segala jenis ancaman siber