

Sertifikat Penilaian Kesadaran Keamanan Siber

Diberikan kepada:

Bismillah2

D3

Jakarta

Tanggal: 14 May 2025

Hasil Penilaian Kesadaran Keamanan Siber:

Kesadaran Teknis
57.4%

Kesadaran Sosial
54.3%

Skor Keseluruhan
55.8%

Tingkat Kesadaran: Baik

Detail Indikator Kesadaran Teknis:

Indikator	Skor
Syarat dan Ketentuan Instalasi Perangkat/Aplikasi	62.5%
Kata Sandi (Password)	62.5%
Internet dan Wifi	65.0%
Keamanan Perangkat	54.2%
Aduan Insiden Siber Teknis	50.0%
Hukum dan Regulasi Keamanan Siber Teknis	50.0%

Detail Indikator Kesadaran Sosial:

Indikator	Skor
Rekayasa Sosial (Social Engineering)	50.0%
Konten Negatif	50.0%
Aktivitas Media Sosial	55.0%
Aduan Insiden Siber Sosial	66.7%
Hukum dan Regulasi Keamanan Siber Sosial	50.0%

Interpretasi Hasil Penilaian

Karakteristik Tingkat Kesadaran Keamanan Siber

Berdasarkan hasil penilaian, Anda memiliki tingkat kesadaran keamanan siber baik (55.8%). Skor kesadaran teknis Anda adalah 57.4% dan kesadaran sosial 54.3%.

Analisis:

Kekuatan:

Area yang Perlu Ditingkatkan:

Analisis Detail:

Analisis:

Dari jawaban responden, bisa dilihat area yang perlu ditingkatkan adalah:

1. Pemahaman terhadap syarat dan ketentuan suatu aplikasi.
2. Penggunaan password yang aman dan tidak membagikannya kepada orang lain.
3. Pemahaman tentang pentingnya menggunakan website https dan penghindaran membuka link atau attachment sembarangan.
4. Pemasangan dan update antivirus secara rutin.
5. Melakukan backup data dan menonaktifkan posisi geografis perangkat digital ketika tidak digunakan.
6. Pengetahuan tentang layanan pengaduan insiden siber dan aturan tentang informasi dan transaksi elektronik.
7. Pengetahuan tentang hukum yang berlaku dan pentingnya menghindari penyebaran informasi hoax dan SARA.
8. Pentingnya tidak membagikan data pribadi pada media sosial dan melaporkan konten negatif dan aktivitas mencurigakan.

Rekomendasi:

1. TINDAKAN PENTING

- Pemahaman syarat dan ketentuan: Cobalah untuk lebih memahami syarat dan ketentuan sebelum menyetujui, jangan hanya membacanya.
- Penggunaan password: Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol dalam password. Jangan pernah membagikan password anda kepada orang lain.
- Keamanan online: Selalu gunakan website dengan https dan hindari membuka link atau attachment sembarangan.

2. PENGUATAN KEAMANAN

- Antivirus: Pasang antivirus pada perangkat digital dan selalu lakukan update secara berkala.
- Backup data: Lakukan backup data secara berkala dan matikan posisi geografis perangkat digital ketika tidak digunakan.
- Pengetahuan hukum: Pelajari lebih lanjut tentang aturan informasi dan transaksi elektronik serta hukum terkait penyebaran informasi hoax dan SARA.

3. PELATIHAN & PENGEMBANGAN

- Ikuti pelatihan online tentang keamanan siber. Sebagai contoh, BSSN menyediakan pelatihan online gratis yang bisa diakses di <https://www.bssn.go.id/>.
- Ikuti webinar atau diskusi online tentang hukum dan etika di internet.

4. ALAT & SUMBER DAYA

- Gunakan aplikasi penyimpan password seperti LastPass atau KeePass untuk membantu mengelola password.
- Gunakan antivirus terpercaya seperti Avast atau AVG.
- Gunakan fitur backup dan restore yang ada di perangkat digital anda.
- Gunakan Aplikasi pengaduan insiden siber dari BSSN yang bisa diunduh di Playstore atau Appstore.

Rekomendasi Perilaku Siber

Rekomendasi Umum:

['Antivirus: Pasang antivirus pada perangkat digital dan selalu lakukan update secara berkala.', 'Backup data: Lakukan backup data secara berkala dan matikan posisi geografis perangkat digital ketika tidak digunakan.', 'Pengetahuan hukum: Pelajari lebih lanjut tentang aturan informasi dan transaksi elektronik serta hukum terkait penyebaran informasi hoax dan SARA. ']

Rekomendasi Teknis:

- Pemahaman syarat dan ketentuan: Cobalah untuk lebih memahami syarat dan ketentuan sebelum menyetujui, jangan hanya membacanya.
- Penggunaan password: Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol dalam password. Jangan pernah membagikan password anda kepada orang lain.
- Keamanan online: Selalu gunakan website dengan https dan hindari membuka link atau attachment sembarangan.
- Gunakan aplikasi penyimpan password seperti LastPass atau KeePass untuk membantu mengelola password.
- Gunakan antivirus terpercaya seperti Avast atau AVG.

- Gunakan fitur backup dan restore yang ada di perangkat digital anda.
- Gunakan Aplikasi pengaduan insiden siber dari BSSN yang bisa diunduh di Playstore atau Appstore.

Rekomendasi Sosial:

Langkah-langkah Implementasi:

1. Ikuti pelatihan online tentang keamanan siber. Sebagai contoh, BSSN menyediakan pelatihan online gratis yang bisa diakses di <https://www.bssn.go.id/>.
2. Ikuti webinar atau diskusi online tentang hukum dan etika di internet.