

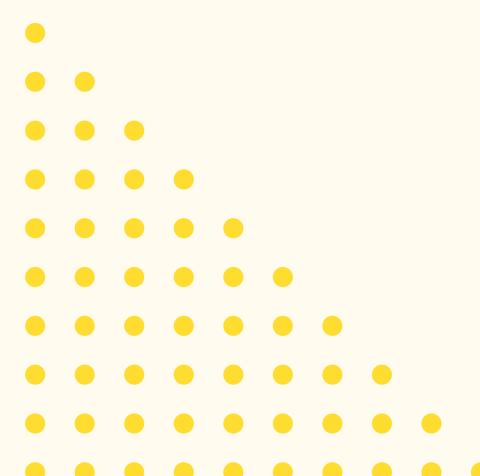
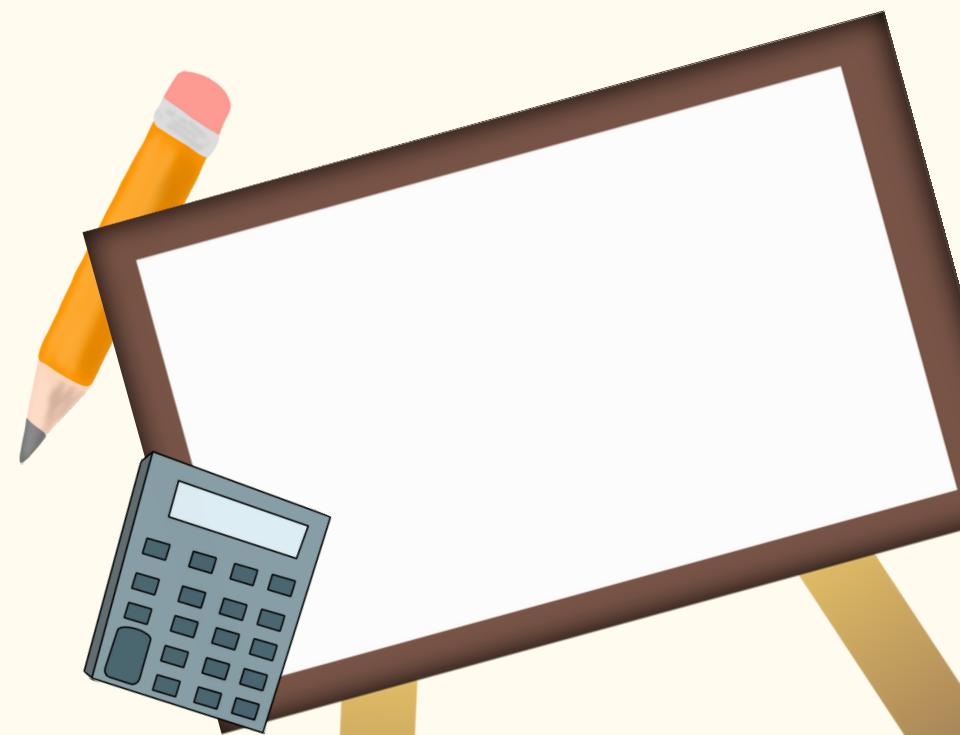
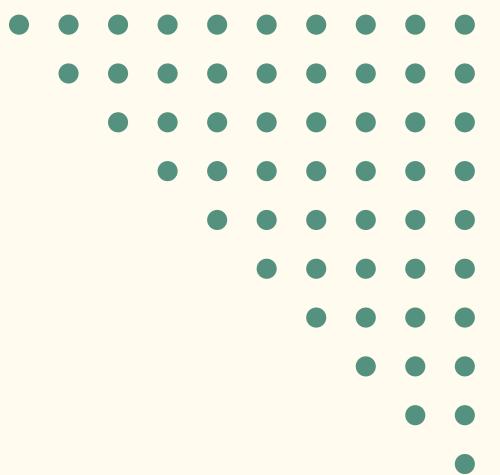


kelompok 2

keamanan sistem

dan proteksi

sistem operasi



Kelompok

2



Arif Frima Ari Suwadji
221011700443



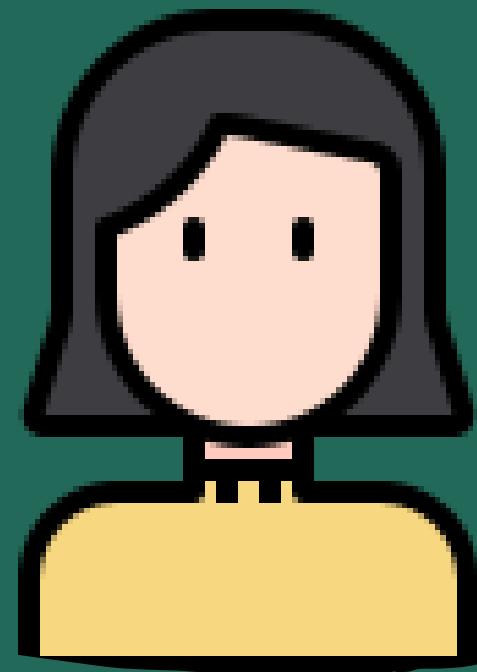
Afrizal



M. Arief Nasar
221011700711



Fauzan fasyah putra
221011700621



Riza fajriah kurnia .P
221011700872



Pendahuluan



Sistem operasi memiliki peran penting dalam menjaga keamanan sistem dan melindungi data dari akses yang tidak sah

Aspek Keamanan Sistem

PERTAMA

Proteksi Memori

- Mekanisme untuk membatasi akses pengguna atau program terhadap area memori sensitif
- Mencegah akses yang tidak sah pada memori yang tidak seharusnya

KEDUA

Proteksi Sumber Daya

- Manajemen hak akses untuk memastikan hanya pengguna yang memiliki izin yang sesuai yang dapat mengakses sumber daya sistem
- Pengaturan kebijakan keamanan

KETIGA

Keamanan Jaringan

- Fitur-fitur keamanan jaringan seperti firewall, pengenkripsi data, dan protokol keamanan
- Melindungi sistem dari serangan jaringan dan akses yang tidak sah

Penyusup/Intruder

1

Hacker

- Seseorang yang mencoba mengakses sistem atau jaringan secara ilegal dengan niat jahat
- Mencuri data sensitif, merusak sistem, atau melakukan kegiatan ilegal lainnya

2

Cracker

- Menggunakan keahlian teknis untuk meretas sistem komputer atau jaringan
- Merusak, mencuri data, atau melakukan kegiatan ilegal lainnya

3

Script Kiddie

- Menggunakan alat dan skrip yang telah dibuat oleh orang lain tanpa pengetahuan teknis mendalam
- Melakukan serangan acak tanpa pemahaman yang mendalam

Autentikasi

Username dan Password

- Metode autentikasi paling umum menggunakan kombinasi username dan password.
- Pengguna harus memasukkan kombinasi yang tepat untuk mengakses sistem.

Kunci Publik dan Privat

- Autentikasi dapat dilakukan menggunakan pasangan kunci publik dan privat.
- Pengguna memiliki kunci privat yang hanya diketahui oleh mereka sendiri, sedangkan kunci publik digunakan untuk memverifikasi identitas pengguna.

Sertifikat Digital

- Sertifikat digital digunakan dalam autentikasi berbasis kunci publik untuk memastikan keaslian dan integritas informasi.
- Diterbitkan oleh otoritas sertifikasi terpercaya.

Pentingnya Keamanan

Sistem Operasi



Penting bagi pengguna dan administrator sistem untuk menjaga keamanan sistem operasi dengan mengikuti praktik keamanan yang baik

seperti mengaktifkan pembaruan keamanan secara teratur, menggunakan sandi yang kuat, dan menginstal perangkat lunak keamanan tambahan jika diperlukan

Selain itu, penting juga untuk memiliki pemahaman yang baik tentang risiko keamanan dan teknik penyusupan yang mungkin terjadi agar dapat melindungi sistem secara efektif.



Keamanan Sistem (lanjutan)

Enkripsi Data

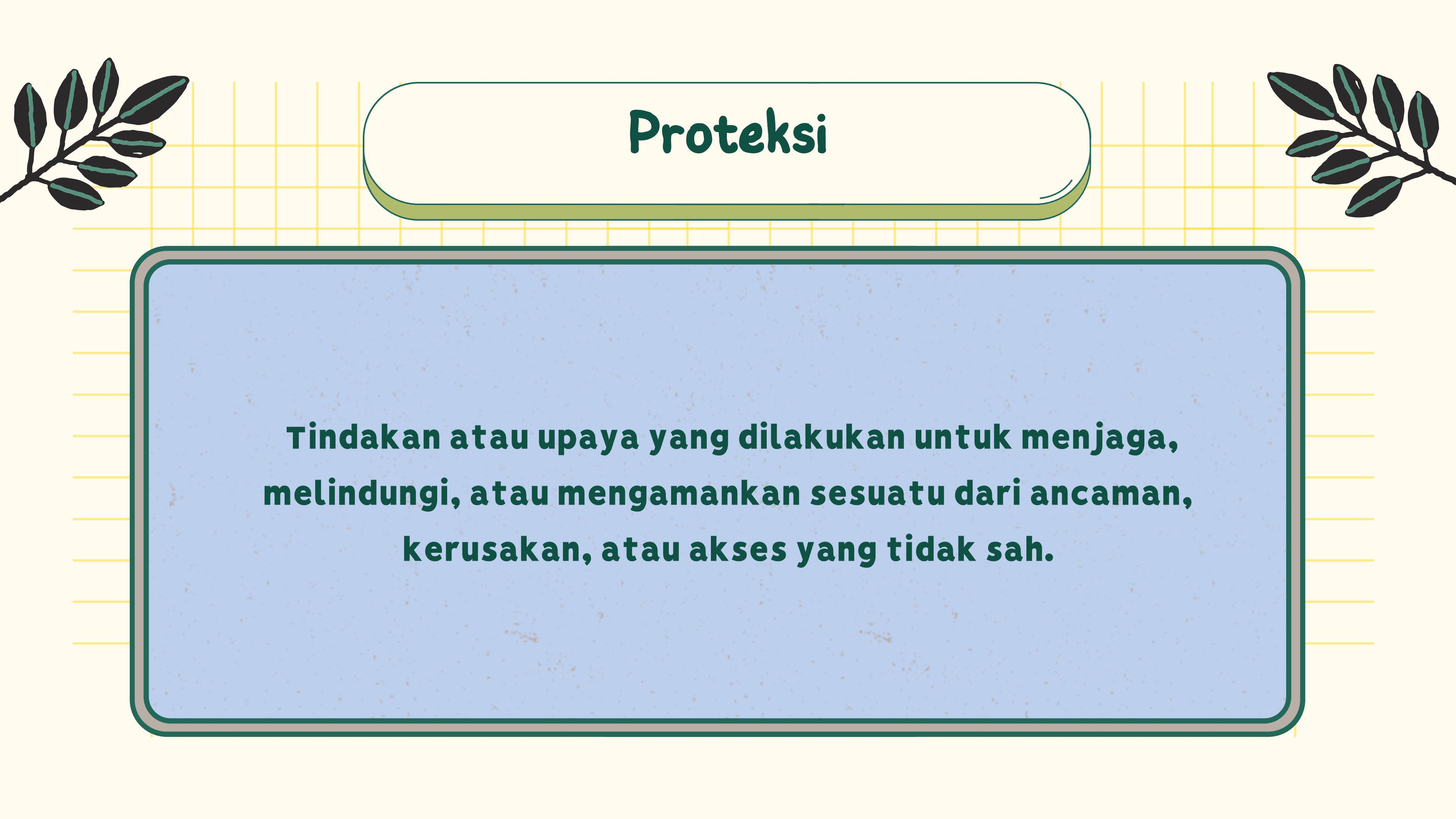
Sistem operasi menyediakan mekanisme enkripsi data yang dapat digunakan untuk melindungi data yang sensitif. Dengan menggunakan enkripsi, data dienkripsi menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang kecuali dengan kunci enkripsi yang tepat.

Log Keamanan

Sistem operasi dapat mencatat aktivitas pengguna dan sistem melalui log keamanan. Log ini dapat berisi informasi seperti log masuk, perubahan konfigurasi, atau upaya akses yang tidak sah. Log keamanan berguna untuk memonitor aktivitas sistem dan mendeteksi potensi pelanggaran keamanan.

Antivirus dan Perangkat Lunak Keamanan

Sistem operasi dapat dipasangi perangkat lunak keamanan tambahan seperti program antivirus, firewall, atau perangkat lunak deteksi intrusi. Perangkat lunak ini membantu melindungi sistem dari ancaman virus, malware, serangan jaringan, atau serangan lainnya.



Proteksi

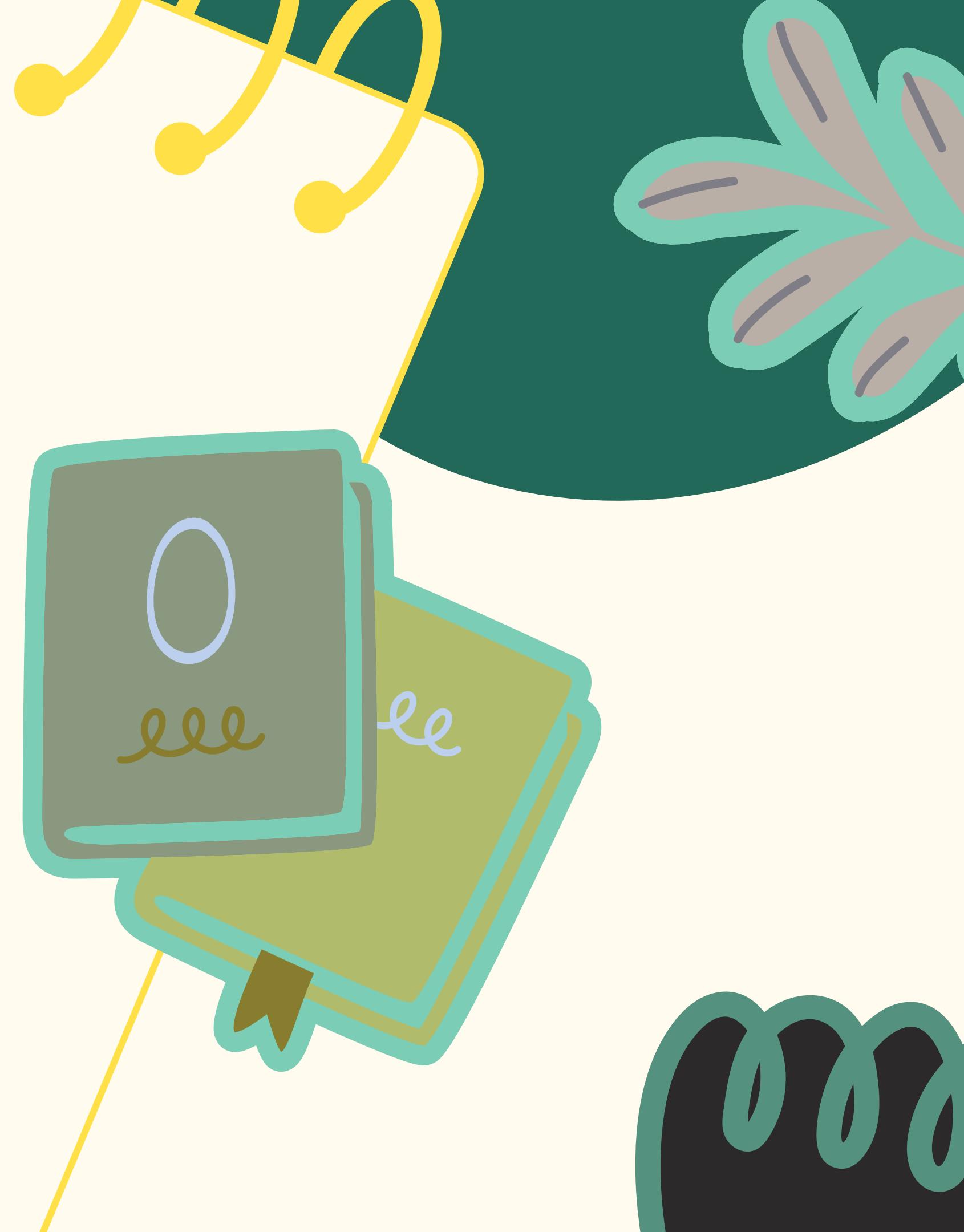
Tindakan atau upaya yang dilakukan untuk menjaga, melindungi, atau mengamankan sesuatu dari ancaman, kerusakan, atau akses yang tidak sah.

**Aspek proteksi dalam menjaga
keamanan sistem operasi.**



Hak Akses Pengguna

Sistem operasi menyediakan mekanisme hak akses pengguna untuk membatasi akses terhadap sumber daya sistem seperti file, direktori, atau perangkat keras. Hak akses ini ditetapkan berdasarkan peran dan tingkat kepercayaan pengguna, sehingga hanya pengguna yang diizinkan yang dapat mengakses sumber daya tersebut.



Multi-Pengguna

Sistem operasi yang mendukung multi-pengguna memungkinkan pengguna untuk memiliki akun pengguna terpisah dengan hak akses yang terbatas. Ini membantu memisahkan data dan lingkungan pengguna, sehingga setiap pengguna tidak dapat mengganggu pengguna lain atau merusak sistem.

Pembaruan Keamanan



Sistem operasi secara teratur menerbitkan pembaruan keamanan untuk memperbaiki kerentanan yang diketahui dan meningkatkan keamanan sistem. Pengguna harus memastikan sistem operasi mereka diperbarui dengan pembaruan terbaru untuk menjaga keamanan sistem dari ancaman yang baru muncul.

Kesimpulan

Dalam pengelolaan keamanan sistem, penting untuk menerapkan praktik-praktik keamanan yang baik, seperti menggunakan kata sandi yang kuat, menjaga perangkat lunak terbaru dengan pembaruan keamanan, membatasi akses terhadap sumber daya yang sensitif, dan memonitor aktivitas sistem secara berkala. Selain itu, pendidikan dan kesadaran pengguna juga penting untuk memastikan tindakan keamanan yang tepat diikuti oleh seluruh pengguna sistem

Daftar pustaka

- Hamzah A. & Suryana A. (2019) Sistem Operasi Informatika**
- Lubis D. & Rostianingsih S (2019) Keamanan Sistem Informasi**
- Tjahyadi B. & Andalas R (2009) Keamanan Jaringan Komputer dan Proteksi Sismtem Informasi**
- Siswanto H. (2010) Hacking: Metode dan teknik Penetrasi Keamanan Jaringan**
- Heryanto T (2018) Autentikasi dan Otorisasi Sistem Informasi**
- Husaini A. (2020) Konsep Dasar Kemanan Jaringan Komputer**

Terimakasih

