



MENGENAL BOT DALAM KEAMANAN INFORMASI

BOT merupakan "robot software" yang dijalankan oleh serangkaian instruksi dalam sebuah kode program untuk dapat berinteraksi dengan website, aplikasi, atau pengguna lain. BOT bisa melakukan pekerjaan berulang-ulang dengan cepat, bisa mengambil alih komputer, dapat dijalankan dalam jumlah yang banyak sekaligus, serta membentuk sebuah jaringan komputer yang dikendalikan (Botnet).



BOT Baik

Digunakan untuk membantu pencarian informasi, chatbot layanan, atau otomatisasi tugas.

Contoh:

- BOT untuk layanan pelanggan.
- BOT untuk pencarian data di internet.

Dalam keamanan informasi, BOT dapat menjadi ancaman karena:

- Menginfeksi perangkat (komputer/HP) tanpa disadari.
- Mencuri data penting, baik data pribadi maupun data instansi pemerintah.
- Membuat botnet (jaringan komputer terinfeksi) yang bisa digunakan untuk serangan besar.
- Mengganggu layanan publik digital, misalnya dengan serangan DDoS hingga aplikasi tidak bisa diakses.
- Menyebarkan spam, hoaks, dan malware secara masif.

BOT Jahat

Digunakan untuk kegiatan ilegal atau merugikan, misalnya mencuri data atau menyebarkan virus.

Contoh:

- Spam BOT: menyebarkan email sampah.
- Social Media Manipulation BOT: menyebarkan disinformasi, menciptakan like/follow palsu dan manipulasi opini publik.
- Click Fraud BOT: memanipulasi jumlah klik pada iklan daring.
- Spy BOT: mengumpulkan informasi dari pengguna tanpa izin.
- DDoS BOT: menyerang server agar layanan tidak bisa diakses.



DISKOMINFOS PROVINSI BALI

PROGRAM LITERASI KESADARAN KEAMANAN SIBER

Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di <https://balikom.info/kabarlentera>



SECURITY
IS INCOMPLETE WITHOUT U
#JagaRuangSiber



**SAYA
NETIZEN
CERDAS**



Dokumen ini telah ditandatangani secara elektronik (TTE).
Scan/Klik QR Code untuk informasi TTE.
Upload file pada <https://tte.komdigi.go.id/verifyPDF> untuk cek keaslian file.

