

# ***Ransomware dan Cara Pencegahannya***



## ***Apa itu Ransomware?***

Ransomware adalah berasal dari nama kelas malware yang terdiri dari dua kata “ranson” yang berarti tebusan dan “malware.” Badan Siber dan Sandi Negara menjelaskan tujuan ransomware adalah menuntut pembayaran untuk data atau informasi pribadi yang telah dicuri. Secara lengkap nya Ransome merupakan jenis malware tertentu yang menuntut tebusan finansial dari korban dengan cara mengancam akan mempublikasikan, menghapus, atau menahan akses ke data pribadi yang penting.

---

## Lalu apa saja jenis Ransomware?

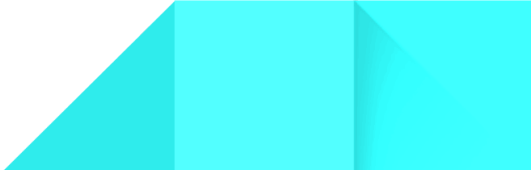
terdapat beberapa jenis ransomware diantaranya yaitu :

1. Crypto ransomware  
Crypto ransomware merupakan serangan dengan merayapi computer atau jaringan untuk mendapatkan informasi penting yang dibutuhkan. Pada jenis ini biasanya akan mengumpulkan dokumen seperti PDF, spreadsheet, gambar dan lainnya kemudian akan dilakukan enkripsi agar kita tidak dapat mengakses data tersebut, kemudian malware akan memaksa kita untuk membayar agar dapat mengakses data tersebut.
2. Locker ransomware  
Jenis ini akan mengunci semua yang ada pada computer sehingga tidak hanya dokumen saja.
3. Scareware  
Scareware berusaha menciptakan kepanikan dengan mengirim notifikasi infeksi virus palsu ke perangkat. Dengan begitu, para pelaku kejahatan siber dapat memanfaatkan kepanikan untuk mendapatkan uang.
4. Doxware  
Doxware adalah jenis ransomware yang mengancam untuk merilis data pribadi kepada publik jika pengguna tidak membayar uang tebusan.

---

## Bagaimana cara kita menjaga keamanan perangkat dari ransomware?

Beberapa tips berikut ini dapat anda lakukan untuk mencegah ransomware

1. Lakukan instalasi antivirus terbaik yang dilengkapi dengan perlindungan ransomware
  2. Mutakhirkan setiap saat antivirus anda serta semua system penting lainnya
  3. Lakukan pencadangan data penting anda pada jaringan atau perangkat lain
  4. Hindari situs web yang mencurigakan dan tidak dapat dipercaya
  5. Jika ingin mengunduh aplikasi lakukan hanya pada marketplace resmi
  6. Jangan mengunduh lampiran email jika anda tidak mengetahui isinya apa dan siapa pengirimnya
- 

---

## Lalu bagaimana jika perangkat kita telah terinfeksi ransomware?

1. Usahakan jangan tergesa-gesa untuk membayar tebusan yang diminta, karena ini hanya akan mendorong penjahat untuk melakukan penipuan kembali
2. Lakukan pemutusan jaringan untuk melindungi komputer lain, karena ransomware dapat menyebar ke komputer lain di jaringan
3. Hapus ransomware secepat mungkin untuk meminimalkan kerusakan.
4. Cari Kunci Dekripsi Online
5. Hubungi Profesional (Dan Mungkin Penegak Hukum)
6. Bangun pertahanan yang Tangguh dengan menerapkan penanganan email, unduhan, dan perilaku menjelajah internet yang aman serta Instal antivirus papan atas