



CYBER CRIME



Pendahuluan

- Perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis Teknologi Informasi dan Internet.
- Jenis-jenis Cyber crime
 - Berdasarkan jenis aktivitasnya.
 - Berdasarkan motif kegiatannya.
 - Berdasarkan sasaran kejahatannya.



Karakteristik Cyber crime

- Terdapat sistem komputer yang terhubung dengan jaringan.
- Pelaku tindak pidana sulit terjangkau.
- Tidak meninggalkan bekas secara fisik, namun dalam bentuk data elektronik.



Karakteristik Cyber crime

- Dilakukan melalui jaringan sistem informasi baik privat maupun publik.
- Tidak menimbulkan kekacauan yang mudah terlihat.
- Kerugian yang ditimbulkan dapat bersifat material maupun non-material, seperti: waktu, nilai, jasa, uang, barang, harga diri, martabat bahkan kerahasiaan informasi.





Berdasarkan jenis aktivitasnya

1. Unauthorized Access.

Terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin dan sepengetahuan dari pemilik sistem yang dimasukinya.

2. Illegal Contents.

Memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum.





Berdasarkan jenis aktivitasnya

3. Penyebaran virus.

Biasa terjadi pada jaringan Internet, Email dan Transferring File (Download).

4. Data Forgery.

Memalsukan data pada dokumen-dokumen penting yang ada di Internet. Biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.





Berdasarkan jenis aktivitasnya

5. Cyber Espionage.

Memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan. Dapat juga membuat gangguan, merusakkan atau penghancuran terhadap suatu data.

6. Cyberstalking.

Kejahatan yang menyerupai teror kepada seseorang dengan memanfaatkan media Internet, seperti mengganggu atau melecehkan.





Berdasarkan jenis aktivitasnya

7. Carding.

Pencurian nomor kartu kredit yang digunakan dalam transaksi internet.

8. Hijacking

Pembajakan hasil karya orang lain, seperti Software, dokumen, file, dsb.

9. Cyber Terrorism

Mengancam pemerintah atau warganegara, termasuk mengganggu ke situs pemerintah atau militer..





10. Hacker (Peretas)

- Suatu kegiatan yang dilakukan untuk menyusup, masuk, dan ikut terlibat ke dalam suatu sistem komputer, jaringan.
- Mencari titik kelemahan dari sebuah sistem jaringan yang akan disusupi dan mulai masuk dan menyusup ke dalam sistem atau program tersebut.
- Aktivitas akhir yang dilakukan oleh Hacker akan menjadi pembagian jenis-jenis Hacker tersebut.





Jenis-Jenis Hacker

- **White Hat Hacker**

Hacker yang tidak memiliki tujuan merugikan.

Biasa menguji ketahanan sebuah sistem yang ia terobos.

Banyak dari mereka yang disewa sebagai konsultan keamanan.

- **Black Hat Hacker**

Jenis Hacker yang aktivitasnya menerobos sistem keamanan komputer untuk melakukan kerusakan, seperti: menghapus file, pencurian identitas, penipuan kartu kredit, dan berbagi aktivitas merugikan lainnya.

Hacker jenis ini disebut juga sebagai **Cracker**.





Serangan Hacker

Defacing

- Mengubah tampilan halaman situs atau website pihak lain.
- Hal ini biasa dilakukan karena merasa tidak puas atau tidak suka kepada individu, kelompok, atau instansi tertentu sehingga website yang terkait dengannya menjadi sasaran utama.

Phising

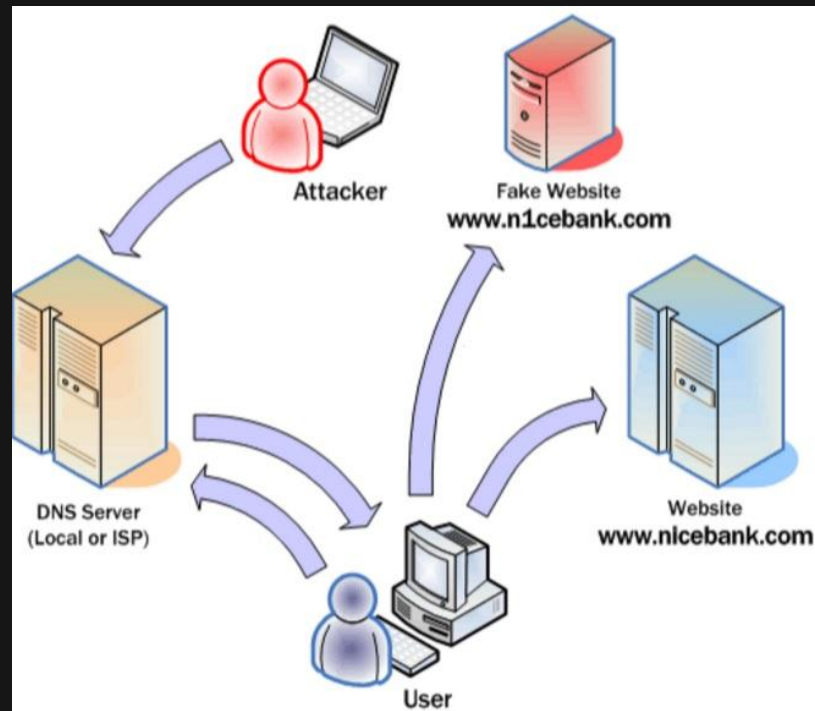
- Memancing user agar mau memberikan informasi seperti username dan password pada suatu website yang sudah di-deface.
- Membuat rujukan alamat-alamat (link) yang mengarahkan browser kita ke alamat web phising atau web palsu.



Serangan Hacker

Pharming

- Suatu cara yang digunakan untuk mengarahkan pengguna situs tertentu untuk masuk ke situs palsu yang mana interface dari situs itu dibuat mirip sekali dengan situs asli.





Berdasarkan Motif Kegiatannya

- Sebagai tindakan murni kriminal.

Sama seperti tindak kriminal lainnya, namun dengan memanfaatkan Internet dan Teknologi Informasi sebagai media kejahatannya.

- Sebagai kejahatan “abu-abu”

Cukup sulit menentukan apakah itu merupakan tindakan criminal atau bukan, mengingat motif kegiatannya terkadang bukan untuk berbuat kejahatan.

Bisa karena iseng atau percobaan.





Berdasarkan Sasaran Kejahatannya

- **Individu**

Sasaran serangan ditujukan kepada perorangan atau individu.

Contoh : Pornografi, Cyberstalking.

- **Hak Milik (Properti)**

Serangan dilakukan untuk mengganggu, mencuri atau menyerang hak milik orang lain.

Contoh: carding, cybersquatting, hijacking, data forgery.

- **Pemerintah**

Tujuan khusus penyerangan pada pemerintah





Pornografi

- Berasal dari bahasa Yunani, yaitu *Porné* yang artinya pelacur dan *Graphein* artinya menulis.
- Pornografi adalah bentuk media komunikasi dan/atau yang dipertunjukkan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat.





Pornografi

- Pornografi dapat berupa: gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, dan gerak tubuh.
- Wujud dari pornografi dapat berupa film, video, VCD, DVD, Hard drive, Flashdisk, Situs Web dan rekaman hand phone dan/atau alat komunikasi lainnya.





Pornografi di Indonesia

- Indonesia Peringkat Dua Pengunduh Pornografi di Internet (tribunnews.com, 2016).
- 25.000 Aktivitas Pornografi Anak Per Hari di Indonesia (kompas.com, 2017).
- 63.066 anak-anak dari 87 juta anak Indonesia terpapar pornografi (dream.co.id, 2018).
- 98,3% Pelajar Terpapar Pornografi (idntimes.com, 2018).
- Mulai 10 Agustus Kominfo Blokir Konten Pornografi di Internet (tempo.co, 2018).





Faktor Penyebab Cybercrime

1. Faktor Teknis

Akses Internet yang *unlimited*.

2. Faktor Politik

Persaingan yang tinggi dan ketat dalam dunia politik, memicu banyak pihak menggunakan kejahatan *cyber* sebagai sarana untuk menjatuhkan pihak lain.





Faktor Penyebab Cybercrime

3. Faktor Sosial dan Budaya

Berkembangnya Teknologi Informasi, kurangnya SDM yang menguasai.

4. Faktor Ekonomi

Perdagangan bebas, rendahnya tingkat ekonomi per individu bahkan suatu negara.





Penanggulangan Cybercrime

- Penggunaan Security Software yang Up to Date.
- Perlunya CyberLaw.
- Kerjasama internasional.
- Perlunya Dukungan Lembaga Khusus.
- Adanya Keamanan Sistem Komputer.



SELESAI