- **Hacking**

  Hacking adalah tindakan tidak sah untuk menyusup atau mengambil alih sistem atau jaringan komputer untuk tujuan tertentu, seperti pencurian data, kerusakan sistem, atau keuntungan finansial.

Jenis-jenis:

- **White Hat Hacking**: Hacker "baik" yang bekerja untuk mengamankan sistem, sering disebut sebagai "ethical hacking."
- **Black Hat Hacking**: Hacker "jahat" yang bertujuan untuk merusak, mencuri data, atau memperoleh keuntungan.
- **Grey Hat Hacking**: Hacker yang kadang-kadang melanggar hukum, tapi tidak dengan maksud jahat, seperti mengekspos kelemahan keamanan sistem.

Contoh Kasus:

- Phishing adalah upaya penipuan untuk mencuri informasi sensitif, seperti username, password, dan informasi kartu kredit, dengan cara menyamar sebagai entitas terpercaya.

- **Phishing**

  Phishing adalah upaya penipuan untuk mencuri informasi sensitif, seperti username, password, dan informasi kartu kredit, dengan cara menyamar sebagai entitas terpercaya.

Jenis-jenis:

- **Email Phishing**: Mengirim email yang tampak resmi untuk mencuri data.

- **Spear Phishing**: Target lebih spesifik dan menyesuaikan pesan untuk individu atau perusahaan tertentu.
- **Whaling**: Mengincar target berprofil tinggi, seperti CEO atau direktur perusahaan.
- **Pharming**: Menyalahgunakan URL untuk mengarahkan pengguna ke situs palsu.

Contoh Kasus:

Serangan PayPal (2014): Penyerang mengirim email yang tampak seperti dari PayPal, meminta penerima untuk memperbarui informasi akun mereka. Banyak pengguna yang mengklik tautan di dalam email dan memasukkan data pribadi mereka di situs palsu, yang mengakibatkan pencurian informasi sensitif.

C. Malware

Malware (malicious software) adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mendapatkan akses ke sistem komputer.

Jenis-jenis:

- **Virus**: Menyebar dengan menginfeksi file lain dan menyebar di komputer atau jaringan.
- **Worm**: Menyebar sendiri tanpa bantuan, biasanya melalui jaringan.
- **Trojan Horse**: Tampak seperti perangkat lunak yang sah tapi sebenarnya berbahaya.
- **Spyware**: Memata-matai aktivitas pengguna dan mencuri informasi pribadi.
- **Adware**: Menampilkan iklan tanpa izin pengguna.

Contoh Kasus:

Fireball (2017): Adware ini menyamar sebagai alat pemasaran, tetapi sebenarnya menginfeksi komputer dan mengalihkan lalu lintas web ke situs-situs tertentu, menghasilkan pendapatan iklan untuk penyerang.

- **Ransomware**

  Ransomware adalah jenis malware yang mengenkripsi data atau mengunci perangkat dan meminta uang tebusan agar korban dapat mengakses kembali data atau perangkat mereka.

Jenis-jenis:

- **Crypto Ransomware**: Mengenkripsi file dan meminta uang tebusan.
- **Locker Ransomware**: Mengunci akses ke perangkat, tapi tidak mengenkripsi file.
- **Scareware**: Mengancam pengguna untuk membayar tebusan dengan memunculkan peringatan palsu.

Contoh Kasus:

Serangan FBI Ransomware (2012): Scareware ini menampilkan pesan yang menyatakan bahwa FBI telah menemukan aktivitas ilegal di komputer pengguna dan meminta pembayaran untuk menghapus 'masa hukuman.' Pesan tersebut menakut-nakuti pengguna untuk membayar tebusan agar tidak menghadapi masalah hukum.