1. **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**:

* Kasus Equifax (2017): Peretasan data besar-besaran yang mengekspos data pribadi 147 juta orang di AS karena kelemahan keamanan dalam sistem perusahaan kredit ini.

1. **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**:

* Kasus phishing Twitter (2020): Beberapa akun Twitter terkenal diretas, termasuk Elon Musk dan Joe Biden, untuk menjalankan skema penipuan Bitcoin.

1. **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**:

* Malware WannaCry (2017): Menyebar secara global dan memengaruhi rumah sakit, bisnis, dan pemerintah, mengunci data pengguna hingga membayar tebusan.

1. **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 ransomware Colonial Pipeline (2021): Menyebabkan kekacauan dalam pasokan bahan bakar di AS setelah jaringan perusahaan minyak ini terkena serangan ransomware oleh grup DarkSide.