**Nama = Muhammad Satriya Pratama M.K.**

**Nim = A11.2022.14225**

**Kelas = A11.4106**

1. **Kejahatan cyber:**

* Ada 4 prioritas utama kejahatan cyber: kejahatan cyber yang disponsori negara (state sponsor actor), kejahatan cyber yang bersifat meneror melalui media cyber (cyberterrorrism), kejahatan cyber yang berbentuk peretasan (malware, cryptolocker, ransomeware) yang bertujuan untuk memeras korban, dan kejahatan cyber lainnya (deface, akses ilegal, penipuan online, ujaran kebencian, permerasan seksual, pornografi anak).
* 5 malware terberbahaya adalah mylebot botnet, phising site, mining pool, VPN gratis yang tidak terjamin, dan netcore backdoor.
* Ada 2 bentuk tindak pidana cyber: computer crime (komputer sebagai objek dan subjek) dan computer related crime (sistem dan pengguna sebagai objek, komputer sebagai subjek).
* Karakteristik kejahatan cyber meliputi modus berbasis IT, alat bukti berupa digital evidence, sifat borderless yang tidak terpengaruh oleh waktu, ruang, dan jarak, serta proses penyidikan yang melibatkan lab digital forensik dan penanganan perangkat komputer sebagai TKP.
* Ada 5 contoh tindak pidana cyber yang dilakukan dengan menggunakan komputer sebagai objek dan subjek (computer crime), dan 5 contoh tindak pidana cyber yang dilakukan dengan menggunakan sistem dan pengguna sebagai objek, serta komputer sebagai subjek (computer related crime).
* Ada beberapa undang-undang yang berlaku untuk tindak pidana cyber, antara lain UU ITE tentang ilegal konten, perjudian, pencemaran nama baik, ancaman pemerasan, dan penipuan online, serta UU ITE tentang ilegal access, ilegal interception, gangguan data, gangguan sistem, penyalahgunaan perangkat, dan pemalsuan identitas.
* Kejahatan cyber dapat menyebabkan terjadinya connect-dependent-vulnerable, yaitu terhubungan dengan teknologi, tergantung pada teknologi, dan rentan terhadap kejahatan.

1. **Modus kejahatan cyber:**

* Ada beberapa modus kejahatan cyber yang sering terjadi, antara lain malware, phising, mining pool, VPN gratis yang tidak terjamin, dan netcore backdoor.
* Modus kejahatan cyber juga dapat berupa data breach dan data leak, yaitu pembobolan dan penyebaran (bocor) data secara ilegal, serta DDoS (distributed denial of service) yaitu serangan yang dilakukan dengan cara mengirimkan jumlah permintaan yang besar ke sebuah server untuk mengakibatkan terjadinya kegagalan atau gangguan dalam sistem.
* Modus kejahatan cyber lainnya adalah deface, yaitu merubah tampilan suatu website dengan maksud terselubung, serta penipuan online yang bertujuan untuk menipu korban dengan menggunakan media internet.

1. **Cara menghindari atau menanganinya:**

* Menggunakan antivirus yang terpercaya dan memperbarui secara berkala.
* Menghindari mengklik link yang tidak dikenal atau mengunduh file dari sumber yang tidak terpercaya.
* Menggunakan password yang kuat dan tidak mudah di tebak.
* Mengaktifkan fitur keamanan pada perangkat seperti firewall dan enkripsi data.
* Menjaga kerahasiaan data pribadi dengan tidak memberikannya kepada pihak yang tidak dikenal.
* Melakukan backup data secara teratur untuk menghindari kehilangan data yang penting.
* Menyimpan data di tempat yang aman dan tidak mudah diakses oleh pihak yang tidak berwenang.
* Mengikuti kebijakan keamanan yang ditetapkan oleh perusahaan atau instansi tempat bekerja.
* Melaporkan ke polres terdekat.