Segurança da Informação

**Hacker**

**Definição:** Pessoa com grande conhecimento em informática, redes e sistemas, que usa habilidades para explorar, melhorar ou testar tecnologias.

**Intenção**

* Ajuda empresas a encontrar falhas e corrigir vulnerabilidade.
* Promove inovação, liberasse de informação e segurança digital.

**Cracker**

**Definição:** Pessoa que usa conhecimento técnico para fins maliciosos ou ilegais, como invadir sistemas, roubar dados ou causar prejuízo.

**Intenção**

* Prejudicar pessoas ou organizações
* Roubar informações, aplicar golpes, quebrar proteções
* Espalhar malwares

**Tipos de ataques**

Engenharia social: é a forma de conseguir informações sigilosas por meio de enganação ou exploração da confiança das pessoas.

Phishing: é quando o golpista pode tentar se passar pela comunicação oficial de uma instituição conhecida.

É o tipo mais simples de ciberataque e, ao mesmo tempo, o mais perigoso e eficiente.

Vulnerabilidades (DDOS): refere-se a uma fraqueza ou falha em um sistema, aplicativo, rede ou processo que pode ser explorada por ameaça para comprometer a integridade, confidencialidade ou disponibilidade de dados.

Malware: programa ou parte de um programa de computador que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Cavalo de Troia: é um veiculo para atacantes ocultos. Este tipo de malware se infiltra no dispositivo da vitima apresentando-se como software legitimo. Uma vez instalado, o cavalo de Troia é ativado.

Ransomware: é a versão do malware da carta de resgate de um sequestrador. Normalmente, ele bloqueia ou nega o acesso ao dispositivo e arquivos ate que ele receba um resgate. Pessoas ou grupos que armazenam informações vitais em seus dispositivos correm risco com a ameaça de ransomware.