TRAINING DAY 2 REPORT

1 JULY 2025

Understand Cybercrime, Hacking and Hacker

Today , I learned some important concepts:

- ## Cybercrime:

  Cybercrime refers to criminal activities that involve the use of computers, digital devices, or networks. These crimes can target computer systems directly or use them as tools to commit other offenses.

  ## Types of cybercrime:

  1. Computer Fraud: The use of computers or digital devices to deceive others for personal or financial gain.

  2. Privacy Violation: Unauthorized access, use, or sharing of someone's personal data.

  3. Identity Theft: Stealing personal information from somebody and impersonating that person.

  4. Electronic Fund Transfer: Illegally accessing or altering electronic transactions to steal money.

  5. ATM Fraud: The unauthorized use of an automated teller machine (ATM) to withdraw money or steal personal banking information, often through methods like card skimming, PIN theft, or machine tampering.

  6. Spam**:** Unsolicited and often irrelevant or inappropriate messages sent over the internet, typically to a large number of users.

- ## History Of Hacking

Hacking began in the 1960s as a term used by computer enthusiasts at institutions like MIT, where early "hackers" explored and modified computer systems for learning and innovation. During the 1980s, with the rise of personal computers, hacking shifted toward unauthorized access and cybercrime, prompting laws like the U.S. Computer Fraud and Abuse Act. The 1990s saw hacking expand globally with the internet, leading to the rise of hacktivist groups and government-targeted attacks. In the 2000s, cybercrime became more organized, involving identity theft, phishing, and state-sponsored cyber espionage. By the 2010s, large-scale data breaches and ransom ware attacks became widespread. Today, hacking includes advanced techniques using artificial intelligence, deep fakes, and plays a significant role in cyber warfare and international conflict.

- # What is Hacking

Hacking is the act of gaining unauthorized access to computer systems, networks, or data. It can be done for various purposes, such as stealing information, causing damage, disrupting services, or exploring systems out of curiosity. While some hackers use their skills maliciously (called **black hat hackers**), others use them ethically to improve security (**white hat hackers**).

- # Who Is a Hacker

A **hacker** is a person who uses their knowledge of computers, programming, and networks to access systems, often bypassing security measures. Hackers can have different intentions:

- **White Hat Hacker** – Uses skills ethically to find and fix security flaws.
- **Black Hat Hacker** – Breaks into systems for malicious or illegal purposes.
- **Grey Hat Hacker** – Hacks without permission but not for personal gain; intentions may be mixed.