□ Slide 1:

Topic: Viruses and Worms

1. □ Definition:

A **computer virus** is a type of malicious software (malware) that replicates itself by attaching to other programs or files. It spreads from one computer to another, often without the user's knowledge or consent, causing damage or disruption to the infected system. A **computer worm** is a type of self-replicating malware that spreads across networks, often without needing to attach itself to other files. Unlike viruses, worms operate independently.

2. □ Simple explanation:

Imagine your computer is like your body. A virus is like a tiny, harmful organism that invades your body and starts making copies of itself, making you sick. It might slow down your body's functions (your computer's performance), or even damage your organs (your computer's files). A worm, on the other hand, is like a mischievous creature that crawls around your house (your network) making copies of itself and causing trouble in different rooms (different computers) without necessarily infecting anything directly. Both can make you (your computer) very unwell.

3. □ Real-life example or analogy:

* **Virus:** Think of a cold. You catch it from someone else (infected file or email), it makes you sick (slows down your computer), and you have to take steps to get better (run antivirus software). The virus replicates itself (the code spreads) when you share files with others (send infected emails or use infected USB drives).

* **Worm:** Imagine a swarm of locusts descending on a field of crops (your network). They don't necessarily attach themselves to individual plants (files) but their sheer number and consumption (replication and network traffic) destroy the whole field (network performance and functionality). A worm can spread rapidly across a network by exploiting security vulnerabilities, crippling multiple computers simultaneously, without needing to infect individual files directly like a virus.

□ Slide 2:

1. □ Definition:

A hacker is an individual who uses their technical skills to gain unauthorized access to computer systems, networks, or data. This access can be achieved through various methods, exploiting vulnerabilities in software, hardware, or security protocols. Hackers may have malicious intent (e.g., stealing data, disrupting services, causing damage) or benign intentions (e.g., ethical hacking to identify vulnerabilities for security purposes). The term "hacker" is often misused and conflated with "cracker," which specifically refers to those who use their skills for malicious purposes.

2. □ Simple explanation:

Imagine a house with a lock on the door. A hacker is someone who figures out how to open that door without the key, either by picking the lock, finding a hidden key, or even finding a way to get in through a window. They might do this to steal something valuable inside (like data or money), to vandalize the house (damage the computer system), or even just to see if they *can* get in.

3. □ Real-life example or analogy:

* **Malicious Example:** A hacker gains access to a company's server containing customer credit card information, stealing the data and selling it on the dark web. This is analogous to a burglar breaking into a store and stealing cash registers.

* **Benign Example (Ethical Hacking):** A cybersecurity company hires a "white hat" hacker to try and break into their own systems to identify security weaknesses before malicious actors can exploit them. This is like a locksmith testing the security of a door lock to ensure it's strong and can't be easily picked.