Tutorial No: 3

Title: Inside the World of Cybercrime: A Closer Look at Two Major Threats with Video Demonstrations

Tutorial Objective: To provide students with a comprehensive understanding of two significant cybercrimes by examining their mechanisms, impact, and real-world examples, supplemented with video demonstrations to enhance learning and retention.

Tutorial Outcome: Students will be able to identify and explain the key characteristics of the two cyber crimes discussed, understand their implications, and recognize preventive measures to mitigate such threats in a practical context.

Maps to Course Outcome – CO2

Bloom Learning Level: Analysis

Instructions: Prepare a PowerPoint presentation on any two cybercrimes (other than in tutorial 2), to explain in detail as a presentation. Also download its related video to demonstrate it in the class.

Presentation Case Study 1:

Title: *Distributed Denial of Service (DDoS) Attack on Google Cloud*

Presenter: Onkar Malawade

- **Introduction to Cybercrime**
- **Overview of Cybercrime**:
  - Cybercrime includes illegal activities involving digital networks or devices, often targeting individuals or businesses.
  - Common cybercrime types include phishing, ransomware, hacking, and denial-of-service (DoS) attacks.
- **Introduction to Selected Cybercrimes**:
  - Denial-of-Service attacks, specifically Distributed Denial-of-Service (DDoS), are one of the most destructive cyberattacks. They aim to overwhelm a server or service with fake traffic, disrupting normal operations.

- **Cybercrime Type**: *Distributed Denial of Service (DDoS) Attack*A DDoS attack floods a network or service with massive amounts of traffic, effectively causing a shutdown by overloading resources.

- It is often carried out using a botnet—a network of infected devices controlled by attackers.

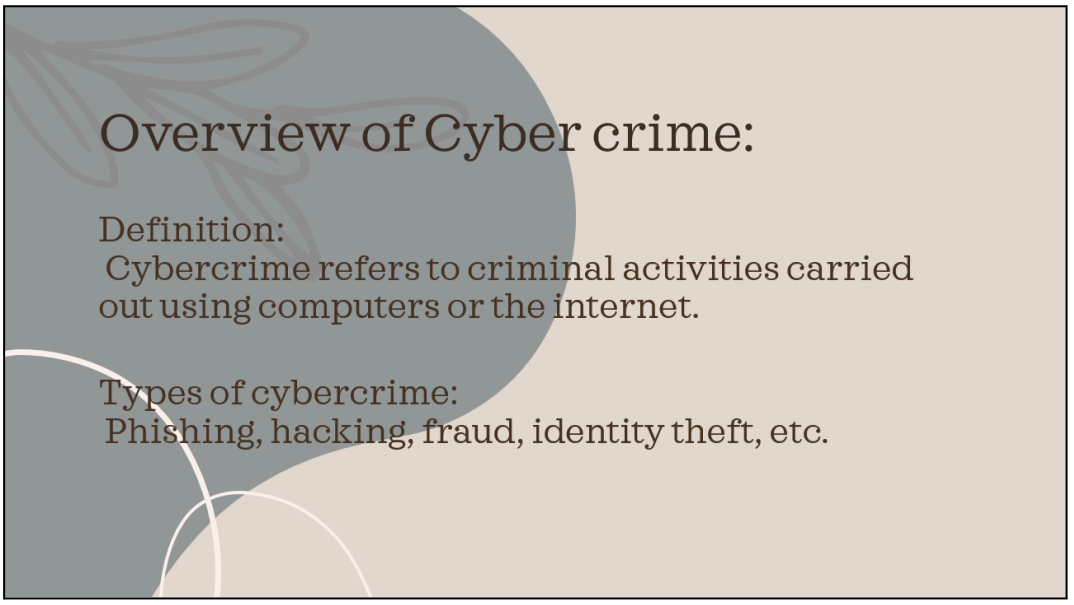
- **How the DDoS Attack on Google Cloud Worked**:

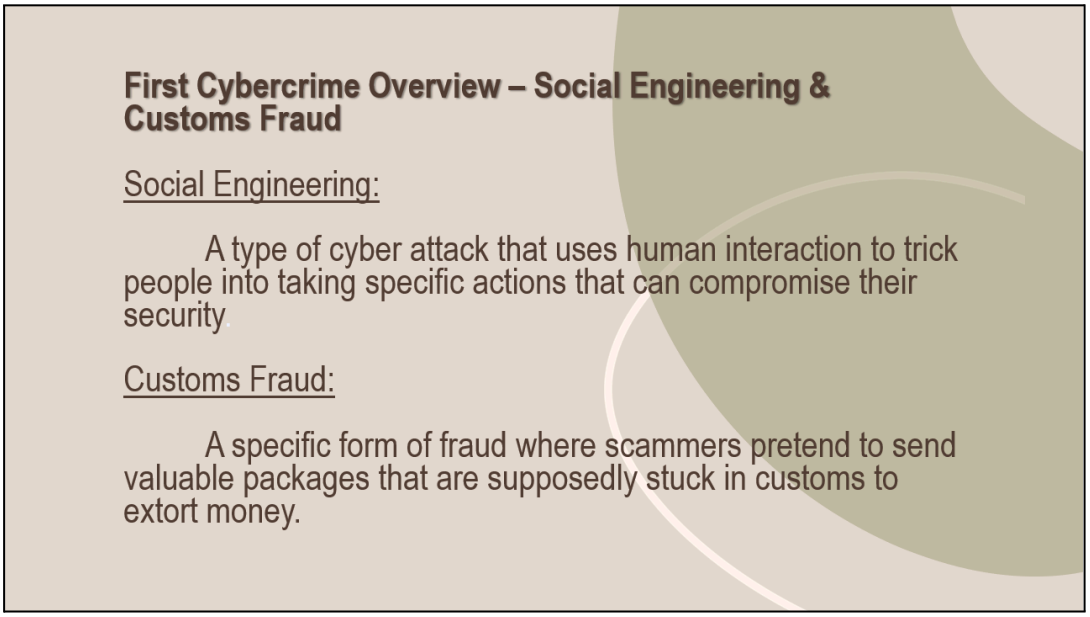
1. Attackers orchestrated a massive Distributed Denial of Service (DDoS) attack against Google Cloud services in October 2023.
2. The attack peaked at an unprecedented 398 million requests per second (rps), making it the largest DDoS attack ever recorded.
3. Some traffic was detected as originating from a botnet created by the **Mirai malware**, which had compromised over 500,000 internet-connected devices.

- **Mechanism of the First Cybercrime (Continued)**
- **Key Elements of the DDoS Attack**:
  - **Botnets**: The Mirai malware had infected over 500,000 devices, which were remotely controlled by attackers to send massive amounts of traffic to Google Cloud's servers.
  - **Overwhelming Traffic**: The sheer volume of 398 million requests per second was more than seven times larger than any previously recorded DDoS attack.
  - **Mitigation**: Google's robust defense systems were able to detect and mitigate the attack, preventing significant damage to its services.

- **Google Cloud DDoS Attack (October 2023)**
- **Real-World Example**:
  - In October 2023, Google successfully mitigated the largest DDoS attack in history, which peaked at 398 million rps.
  - The attack involved a botnet powered by **Mirai malware**, which infected over 500,000 devices connected to the internet.
  - Google's security systems were able to absorb and neutralize the attack, preventing major disruptions to its cloud services.

Presentation Case Study 2:





How the Attack Works:

INITIATION:

THE ATTACKER MAKES CONTACT VIA SOCIAL MEDIA, DEVELOPS A RELATIONSHIP, AND BUILDS TRUST.

FAKE GIFT OFFER:

THE FRAUDSTER PROMISES TO SEND A GIFT FROM ABROAD.

CUSTOMS TRAP:

THE VICTIM IS TOLD THE PACKAGE IS STUCK IN CUSTOMS AND MUST PAY CLEARANCE, INSURANCE, AND OTHER FEES.

- **Detailed Steps**:

Escalating Demands: After initial payments, more money is demanded under various pretenses (insurance, taxes, etc.).

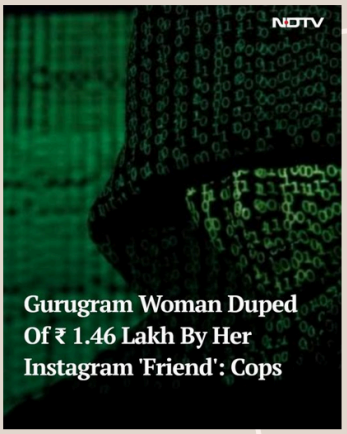
Pressure Tactics: The victim is threatened with penalties if they do not pay (e.g., package can't be returned, legal action).

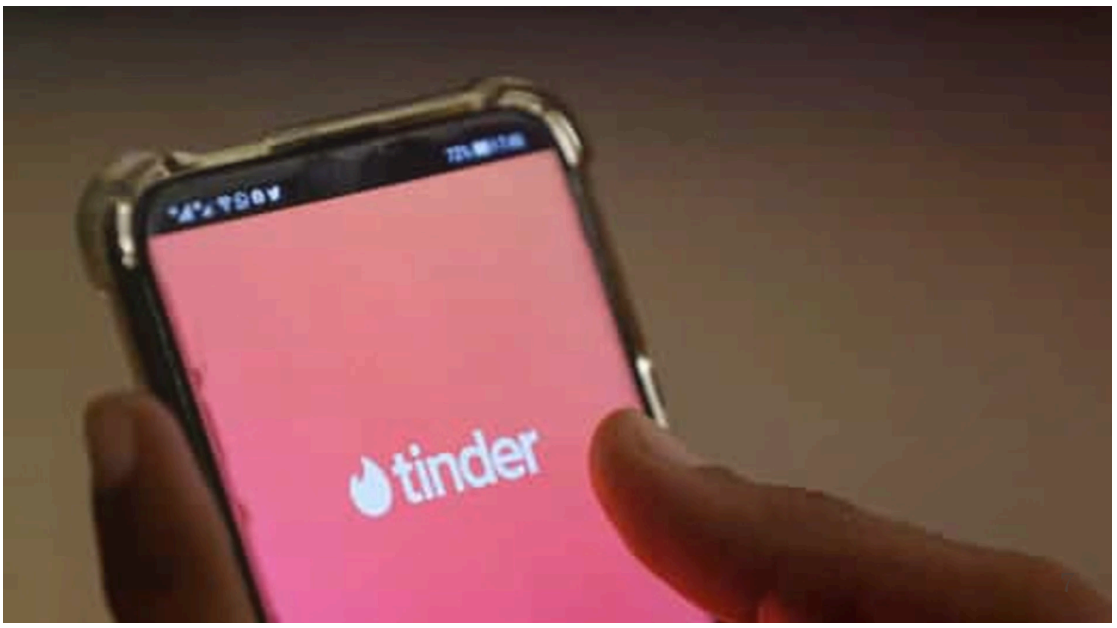
Gurugram Woman Duped of ₹ 1.46 Lakh:

A. Social media contact through Instagram.

B. Scam involving customs fees and escalating demands.

C. Victim lost ₹ 1.46 lakh before contacting the police.





Impact and Consequences of the Cybercrime

- **Financial Impact**: Victim lost significant money (₹ 1.46 lakh).
- **Emotional Impact**: Stress, loss of trust, embarrassment.
- **Legal Consequences**: FIR filed under Bharatiya Nyaya Sanhita (BNS) at Cybercrime Police Station.
- **Prevention Measures**: Public awareness, reporting, and understanding the signs of social engineering.