**Use of Computer Science Technologies**

**and Cyber Crime**

**Group 3 Civics Presentation  
Presented By:  
1. Mursaleen  
2. Waleed  
3. Muhammad  
4. Usman**

**5. Zainab  
6. Fatima**

***Slide 4-5:***

***#04:***

Three core technologies in computer science:

1. **Artificial Intelligence (AI):**
   * AI powers smart devices and enhances decision-making processes across industries. It's used in various applications like automation, data analysis, and machine learning.
2. **Cloud Computing:**
   * Cloud computing enables the remote storage, management, and processing of data. It offers flexibility and scalability, allowing users to access and store data online without relying on local servers.
3. **Internet of Things (IoT):**
   * IoT connects physical devices to the internet, enabling automation and control. These devices can collect and exchange data, improving efficiency and interaction between systems.

***#05:***

The key Benefits of Technology across various sectors:

1. **Efficiency**:
   * Automation of manual processes increases overall efficiency and reduces human error, streamlining workflows and saving time.
2. **Communication**:
   * Technology facilitates real-time communication, enabling global collaboration across different teams and locations, breaking down geographical barriers.
3. **Healthcare**:
   * Advances in technology have improved diagnostics and enhanced patient care, leading to more accurate and timely treatments in healthcare systems.
4. **Data Management:**
   * Technology has revolutionized data handling, improving the management and processing of data, which is especially crucial in industries like healthcare for maintaining patient records and improving outcomes.
5. **Education**:
   * E-learning platforms powered by technology provide widespread access to educational resources, making knowledge more available to people around the world.

***Slide 8-9:***

***#08:***

**How Cyber Criminals Operate**

1. **Social Engineering:** Attackers use tricks like fake emails or phone calls to fool people into revealing sensitive information, like passwords or financial details.
2. **Exploiting Vulnerabilities:** Hackers find and take advantage of weaknesses in software or systems to gain unauthorized access.
3. **DDoS Attacks:** By flooding a target computer or network with too many requests, attackers overwhelm it, causing it to crash or become unusable.
4. **Illegal Data Mining**: Cybercriminals steal valuable data, such as credit card numbers or personal information, often to sell or use for fraud.
5. **Advanced Persistent Threats (APTs):** These are long-term, stealthy attacks where hackers gain access to a system and stay undetected, stealing sensitive information over time.

***#09:***

**Case Studies of Major Cyber Crimes**

* **Equifax Data Breach (2017)**

Hackers exploited a security vulnerability in Equifax's systems, stealing the personal data of 147 million people, including Social Security numbers, addresses, and credit card information. This was one of the largest breaches of sensitive information ever recorded.

* **Yahoo Data Breach (2013-2014)**:

Yahoo suffered two massive breaches, affecting 3 billion accounts in 2013 and 500 million accounts in 2014. Hackers stole names, emails, passwords, and security questions, making it one of the largest data breaches in history.

* **SolarWinds Hack (2020)**:

A sophisticated group, likely backed by a nation-state, compromised SolarWinds' software, allowing them to infiltrate the networks of U.S. government agencies and major corporations. This supply chain attack went undetected for months, posing a severe threat to national security.

* **WannaCry Ransomware Attack (2017)**:

A global ransomware attack affected over 200,000 computers in 150 countries. The malware encrypted files and demanded a ransom in Bitcoin. It severely disrupted hospitals, businesses, and governments, particularly the UK’s National Health Service (NHS).