

**DATABASE SYSTEM PROJECT**

**Submitted by: Muhammad Ammar Kalim (242776)**

**Muhammad Abdullah Nasir (242779)**

**Section: 2B**

**Submitted to: Ms.** **Kainat Nazir**

**Cybersecurity Threat Tracker – Database Project**

**Introduction:**  
The **Cybersecurity Threat Tracker** is a database project that records different types of cyber attacks like phishing and malware. It stores details about the threat, its severity, affected industries, countermeasures taken, and sends alerts for serious threats. This system helps cybersecurity teams quickly track, manage, and respond to attacks in real-time.

## ****Purpose of the Database:****

1. **Store Cyber Threat Data:**  
   Safely store detailed information about different types of cyber threats (phishing, malware, ransomware, etc.).
2. **Track Threat Activities:**  
   Record when, where, and how threats occurred to create a history of incidents.
3. **Analyze Threat Patterns:**  
   Help organizations study past attacks and find patterns (for example: which industry gets attacked most often, or which months have more attacks).
4. **Assist in Faster Responses:**  
   Allow cybersecurity teams to quickly check previous countermeasures and apply better solutions for current/future threats.
5. **Generate Alerts for High-Severity Threats:**  
   Automatically create warnings or alerts if a very serious (critical) threat is detected.
6. **Improve Cybersecurity Strategies:**  
   Organizations can use the database reports to improve their overall security systems.
7. **Academic and Career Development:**  
   Showcase my ability to design and implement a professional-level database system, important for academic success and useful in job applications.

## ****Target Audience:****

1. **Cybersecurity Analysts:**  
   Professionals who detect and investigate cyber attacks will use the database to review threat histories and plan defenses.
2. **IT Departments of Companies:**  
   Internal tech teams can use the database to manage security incidents and prepare better protection systems.
3. **Government Cybersecurity Agencies:**  
   Government units responsible for national cyber defense can study collected threat data to make better public cybersecurity policies.
4. **Researchers and Students:**  
   Individuals studying cyber attacks and digital safety can use the data for academic research, project work, or training purposes.
5. **Company Managers and Executives:**  
   Business leaders can view summarized threat reports to make important financial or security decisions (like investing more in cybersecurity tools).

**Entity-Relationship Diagram**

