S.No	Problem Statement ID	Problem Statement Name	Domain
6	CT-AICS - 02	Phishing Detection Tool	AI Cyber Sec

Description:

The **Phishing Detection Tool** is designed to help individuals and organizations identify and block phishing attempts. Phishing is a type of cyberattack where attackers trick users into revealing sensitive information, such as passwords, credit card numbers, or personal data, by pretending to be legitimate entities through fake emails, websites, or messages.

This tool will analyze suspicious emails, URLs, or messages, identify potential phishing indicators, and alert users about the threat. It can also provide educational feedback on why a message or site is flagged as phishing.

Objectives:

1. **Identify Phishing Attempts:**
    - Analyze emails, messages, or URLs to detect phishing attempts.
    - Flag signs like mismatched domains, fake branding, or suspicious attachments.
2. **Educate Users:**
    - Teach users about phishing tactics by explaining why something is flagged.
    - Help them recognize phishing attempts in the future.
3. **Prevent Damage:**
    - Block malicious links or attachments before users can interact with them.
    - Alert users or administrators about potential threats in real-time.

Expectations:

1. **For Developers:**
   - Build a tool that uses machine learning, pattern recognition, or rule-based systems to detect phishing attempts.
   - Ensure the tool is user-friendly and works seamlessly in email clients, browsers, or as a standalone application.
2. **For End Users:**
   - Provide easy-to-understand warnings when phishing is detected.
   - Offer clear explanations to improve user awareness about phishing tactics.
3. **For Organizations:**
   - Protect employees and systems from falling victim to phishing attacks.
   - Provide analytics and reports to improve security policies and training.

Expected Results:

1. **Accurate Phishing Detection:**
   - Successfully identify phishing emails, websites, and messages with minimal false positives.
2. **User Awareness and Training:**
   - Educate users on phishing tactics and how to avoid them.
3. **Enhanced Security:**
   - Block malicious content, preventing data breaches or financial losses.
4. **Comprehensive Reporting:**
   - Generate reports for organizations on detected threats and user interactions.