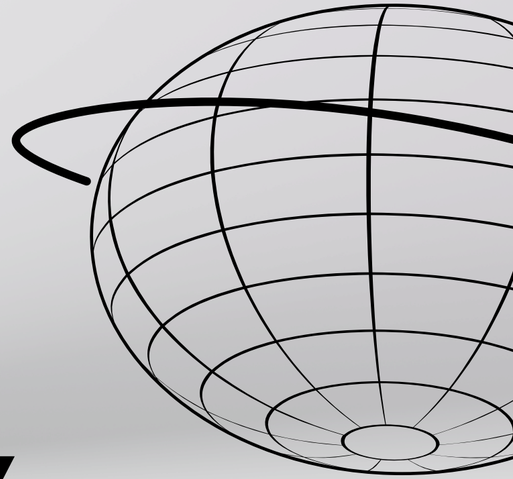
APE SECURITY

AI-Powered Anti-Phishing Detection Browser Extension for Students



PROBLEM STATEMENT

Students are primary targets of:

- Fake internship offers
- Scholarship scams
- Fake hackathon registrations
- Credential harvesting emails

Most phishing attacks:

- Use urgency tactics (“Act within 24 hours”)
- Mimic trusted institutions
- Contain malicious login links

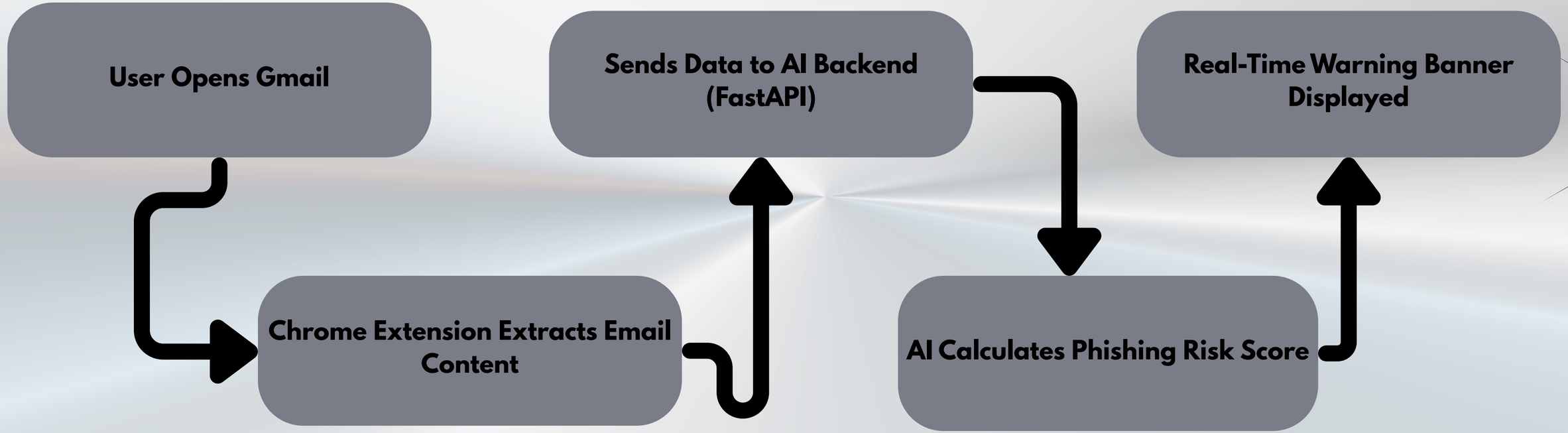
Students often:

- Click without verifying
- Share credentials unknowingly
- Lose personal or financial data

Gap in Existing Solutions:

- Generic spam filters miss student-specific scams
- No real-time warning inside Gmail
- No contextual phishing intent analysis

OUR WORKFLOW



Components

1. **Chrome Extension**
- Runs inside Gmail
- Extracts text & links
- Prevents duplicate scanning
- Displays warning banners

2. **AI Backend**
- Built using FastAPI
- Performs phishing intent analysis
- Generates calibrated risk score (0–100)

AI Detection Logic

Detection Layers

- Phishing intent keywords: - verify account, reset password, login immediately.
- Credential harvesting words: - password, OTP, login.
- Urgency & fear triggers: - urgent, suspend, last warning.
- Suspicious domains: - .xyz, .top, non-HTTPS links.
- Student-targeted scam patterns: - internship offer, scholarship approval, hackathon registration.
- Trusted domain filtering: - .edu, .ac.in → reduce false positives.

Impact & Future Scope

Impact
Prevents credential theft
Reduces student financial fraud
Increases phishing awareness
Promotes cybersecurity hygiene

Future Scope
Integration with CERT-In phishing reporting system
Machine learning enhancement
Institution-level deployment
Mobile email support