Innovation

1) Problem & context

Phishing is still the top initial access vector. Most defenses fall into two buckets:

1. **Enterprise email security gateways/SEGs** (filtering at the mail layer with AI/ML, policies, impersonation protection), and
2. **Security awareness training (SAT)** platforms (simulated phishing + training content).

Representative examples:

- **KnowBe4** — leading SAT platform providing simulated phishing and training at scale. KnowBe4
- **Cofense PhishMe** — SAT with real-world simulations and reporting workflows. Cofense+1
- **Microsoft Defender for Office 365** — anti-phishing policies, spoof/impersonation protection at the mail layer. Microsoft Learn+2Microsoft Learn+2
- **IRONSCALES / Barracuda / Tessian (now Proofpoint)** — AI email security, anomaly detection, BEC protection. coolspirit.co.uk+6ironscales.com+6ironscales.com+6

These tools are primarily organization-centric and either (a) filter mail automatically or (b) run periodic simulations and training. They do not typically provide an **on-demand, user-initiated conversational analysis** experience that educates the individual user with a transparent, step-by-step explanation and personal analytics.

2) ThreatIQ's proposal (what's new)

ThreatIQ is a **user-facing phishing awareness chatbot** that combines:

- **Heuristics** (urgency keywords, sender anomalies, hyperlink/domain checks) with
- **Lightweight threat intel** (WHOIS age, optional VirusTotal lookups), and
- **Generative AI** producing a **structured, explainable verdict** (judgment, explanation, tips),
- Plus a **personal analytics dashboard** (daily/ monthly usage; judgment breakdown).

The emphasis is **education + transparency** for end users: the system shows *why* something looks risky and how to act safely, not just “allow/block”.

3) Market scan & gap analysis

- **SAT platforms (KnowBe4, Cofense)** focus on campaigns and training efficacy at org level; they do not provide a personal, on-demand conversational triage tool integrated with a user’s own history dashboard. KnowBe4+2Cofense+2
- **Email security vendors (Microsoft Defender, IRONSCALES, Barracuda, Tessian/Proofpoint)** intercept threats in transit and provide admin-oriented dashboards; end users typically see banners/quarantine notices rather than explainable chatbot feedback and personal metrics. Proofpoint+6Microsoft Learn+6Microsoft Learn+6
- Academic/industry resources discuss phishing detection broadly, but **a privacy-respecting, explainable, per-user triage chatbot** with lightweight intel + personal analytics is not a mainstream, commoditized pattern.

Conclusion of gap: Our project occupies the space **between** training platforms and mail-gateway products: a **self-service, educational triage companion** for individuals that also builds long-term awareness via personal stats.

4) Category claim (per rubric)

- Because there are many phishing solutions overall, claiming “totally new” would be unrealistic.
- However, the **specific combination—user-initiated conversational triage**, **explainable AI output**, **heuristics + WHOIS/VT context**, and **personal analytics dashboard**—is **not the standard approach** of mainstream tools, which are org-admin or filter-centric.

Claim: Niche (2 pts).
There are clearly multiple good competitors in phishing defense and training, but ThreatIQ applies a distinct, user-centric design and explanation-first workflow that is not the dominant paradigm. This positions the project as a **niche innovation** rather than “common” or merely “trendy”.

5) Why this is valuable

- **Education and behavior change**: explanations + tips improve user judgment over time (beyond a binary block/allow).

- **Transparency**: combines ML reasoning with concrete signals (domain age, mismatched links, urgency wording).
- **Adoption & trust**: a chat interface lowers the barrier to ask, “is this safe?”, encouraging proactive checks.
- **Portability**: the same pattern can extend to SMS, social DMs, or browser extensions.

6) Risks & how we address them

- **False positives/negatives** → mitigate with hybrid signals and conservative language in outputs.
- **Privacy** → store minimal data and keep explainability local to the user; external lookups optional.
- **Over-reliance on AI** → present recommendations as guidance, not absolute verdicts; surface heuristics explicitly.