项目计划书

澄源-基于知识图谱与大模型的反诈新范式

智能反诈演练平台 —— 练出防骗真功夫

澄源团队

目录

一、执行摘要

电信网络诈骗是一个日益猖獗且不断演变的全球性问题，严重威胁着个人财产安全和网络空间的信任。尽管政府和金融机构已推出国家反诈中心 APP、96110 预警劝阻专线、12381 涉诈预警劝阻短信系统、支付安全等等多项措施，综合利用大数据、人工智能、数字安全等技术手段进行防范，但诈骗手段更新快、隐蔽性强、跨地域性突出，传统防范和教育模式面临挑战。 公众，尤其是易受骗群体，需要更有效、更具吸引力的教育方式来提升防范意识和识别能力。 因此，本项目设计了一款集防诈骗模拟演练、主动防御、诈骗教育等功能为一体的智能反诈演练平台。

该平台利用知识图谱、人工智能 (AI) 与机器学习 (ML)、自然语言处理 (NLP)、大型语言模型 (LLM)等技术，实现了诈骗关系网、AI 模拟诈骗实战、主动防御机制、社区互动以及游戏化学习体验等多种立体功能，依此提高了平台对公众的吸引力，以“游戏”的方式教育人们预防各类诈骗手段，并通过提供结构化的反诈知识、沉浸式的实战训练和互助的学习社区，帮助用户轻松无痛地掌握反诈技能，从而增强个体防范能力，弥补现有解决方案在用户参与度和教育有效性方面的不足的问题。

本团队成员具备互联网技术研发与金融数据深度应用等多元化专业背景，通过系统开展市场调研分析，精准洞察行业发展趋势。在对目标市场规模、增长态势以及行业发展机遇的深入研究中发现，当前大众对反诈演练平台存在迫切需求。

在产品竞争力层面，经与市场现有反诈产品横向对比，本团队研发的智能反诈演练平台在 AI 模拟实战、主动防御训练及游戏化学习模式等方面展现出显著优势。同时，基于清晰的品牌定位与明确的营销目标，我们制定了关键绩效指标体系，并规划了多元盈利模式：一方面通过精准投放对应领域广告，另一方面向政府机构、企业客户提供定制化反诈演练服务。此外，我们还对未来 3-5 年的收入与成本进行了科学预测，并针对可能面临的市场、技术等风险，制定了完善的应对策略，确保项目稳健发展。

二、团队简介

“澄源”项目团队是一支充满活力、以在校大学生为主导的创新集体。我们的团队成员主体为在校大学生，他们代表着互联网最活跃的用户群体，对各类新兴网络现象和诈骗手段有着天然的敏感性和深刻的感知。这使得我们在理解目标用户（尤其是年轻群体）的需求、行为模式以及易受骗的心理弱点方面具有独特的优势。我们汇聚了对反电信网络诈骗事业充满热情和使命感的年轻力量，且他们具备扎实的理论基础和快速学习能力能够迅速适应并掌握新技术。团队的核心动力源于对构建更安全数字环境的共同愿景，以及在实践中学习和成长的强烈渴望。我们团队将以知识图谱技术为起点，结合现在的人工智能大模型技术，引入“主动式防御”概念，设计一款新型反诈应用。团队成员名单如下：

姓名	性别	学校	专业	级别	职责
柳秀秀	女	青海师范大学	计算机科学与技术	副教授	指导老师
李垚	男	青海师范大学	园艺	讲师	指导老师
夏雨轩	男	青海师范大学	软件工程	三年级	项目总监 / 架构师
李发渊	男	青海师范大学	软件工程	三年级	技术负责人 / 后端开发主管
范潇宇	男	青海师范大学	软件工程	三年级	数据架构师 / Neo4j 开发
付宇航	女	青海师范大学	软件工程	三年级	财务运营
王生斌	男	青海师范大学	软件工程	三年级	市场
祖少楠	男	青海职业技术大学	软件工程	二年级	数据工程师
姜斌	男	四川大学锦江学院	计算机科学与技术	二年级	内容策划
葛世文	男	东莞理工学院	电气工程及其自动化	四年级	用户体验设计师 / 前端开发

2.1 指导老师介绍

柳秀秀

柳秀秀，博士，副教授，硕士生导师，括软件与网络工程系主任 及教工党支部书记，一直从事模式识别、物联网及无线网络与安全等方向的研究，具备扎实的研究基础和研究能力，目前已在《IEEE Transactions on Communications》（SCI 一区， TOP 期刊，影响因子 7.2）、《电子学报》（CCF A 类）、《IEEE Sensors Journal》（SCI 一区， 影响因子 4.3）、《重庆邮电大学学报（自然科学版）》（CSCD）等国内外知名期刊发表高水平论文 9 篇。授权国家发明专利 1 项，国际发明专利 1 项，申请软著 5 项。主持省部级科研项目和横向项目各 1 项，获得青海省科技进步三等奖、技术发明奖三等奖。她的专业知识和科研能力为“澄源”项目在核心技术研发、知识图谱构建和 AI 模型应用等方面提供关键的学术和技术指导。

李垚

李垚老师同样是青海师范大学计算机学院的重要成员。李老师深度参与计算机学院的各项工作，尤其在党务及行政管理方面扮演着核心角色。

李老师目前担任计算机学院的辅导员及教工党支部副书记。他直接面向学生，负责学生思想政治教育、社团建设和日常管理工作，例如指导学院团总支、学生会的换届工作，并对新团员寄予厚望。同时，他深度参与学院的党建工作，在多次党内学习和专题研讨会中担任领学或主持角色。李老师在学生工作和组织管理方面的丰富经验，将为“澄源”项目的团队建设、用户定位（尤其是学生群体）以及后期运营推广策略的制定提供宝贵的实践指导和资源支持。

2.2 核心团队成员介绍

夏雨轩：项目负责人

- 角色定位： 项目负责人不仅是团队的领导者，更是项目的战略规划者和整体架构师。他负责设定项目目标和方向，确保开发过程与项目愿景保持一致。

他在项目管理方面的经验对于协调各项资源、制定里程碑计划、以及应对项目实施过程中的挑战至关重要。

- 技术贡献： 拥有一定的架构制定经验，这意味着他能从宏观层面设计系统的模块划分、技术选型和系统集成，为“澄源”项目的复杂技术栈（如图数据库、NLP、LLM、前后端应用）奠定稳固基础。同时，他的前后端开发经验确保他对项目的技术实现细节有深入理解，能够指导开发工作，并在必要时亲自参与关键代码的开发。

- 项目相关性：在反诈应用开发中，整体架构的合理性直接影响系统的性能、可扩展性和安全性。项目负责人的技术背景使其能够更好地评估和引入先进技术，例如高性能图数据库 Neo4j 以及 NLP/LLM 在信息抽取和模拟对话中的应用。

李发渊：项目开发团队主要负责人

- 角色定位： 开发团队的主要负责人，李发渊承担着技术落地的核心责任。他负责指导日常开发工作，解决技术难题，确保代码质量和开发进度符合要求。他在多类型项目开发经验积累了处理不同技术栈和项目复杂度的能力。

- 技术贡献： 具备丰富的数据分析经验是李发渊的一大优势。在“澄源”项目中，数据分析能力至关重要，用于从海量反诈信息中识别模式、提炼特征，并将这些信息结构化存储到知识图谱中。他还能利用数据分析优化 AI 模型的训练和反诈策略的效果。

- 项目相关性： “澄源”项目的核心技术之一是基于知识图谱和 AI 进行智能预警和识别。李发渊的数据分析和开发经验能够直接赋能知识图谱的构建、关系的抽取（如诈骗手段、团伙特征、资金流向）以及 AI 模型的训练和部署。

范潇宇：项目开发团队成员

- 角色定位： 作为开发团队的重要成员，范潇宇专注于项目的具体实现，尤其在数据库操作和结构制定方面发挥关键作用。他在数据库领域的专长对于构建和维护项目底层的反诈知识图谱至关重要。

- 技术贡献： 数据库操作和结构制定的经验确保了项目能够有效地存储、管理和查询复杂的反诈知识数据。他负责设计知识图谱的模式（Schema）、优化数据存储方式以及实现高效的数据存取接口，这些是保证知识图谱性能和可用的基础。

- 项目相关性： “澄源”项目以 Neo4j 图数据库为基石来存储诈骗网络关系。范潇宇的数据库经验直接支持了这一核心组件的建设，包括数据建模、索引优化、查询效率提升等工作，确保知识图谱能够支撑智能预警、案件分析和模拟诈骗等功能。

2.3 团队组织架构与分工

项目团队采用了精简高效的组织架构，将职责划分为以下几个核心部门，确保各司其职，高效协作，团队组织架构与分工如下图所示。

图 2.3-1 团队组织架构与分工

项目管理与战略部

- 夏雨轩：项目总监 / 首席架构师
  - 角色定位：作为项目最高领导者，负责项目的整体战略规划、方向制定、资源协调和风险管理。同时，承担首席架构师的职责，宏观设计系统的模块划分、技术选型和集成，确保项目技术路线与业务目标一致。
  - 职责： 制定项目愿景、目标和里程碑；统筹各部门工作，确保项目进度和质量；进行技术栈和系统架构的顶层设计；解决跨部门协作难题；评估和引入前沿技术（如高性能图数据库、NLP、LLM 等）。

技术研发部

- 李发渊：技术负责人 / 后端开发主管
  - 角色定位： 作为技术研发团队的核心领导者，负责后端系统的设计、开发、测试和维护。
  - 职责： 领导后端开发工作，指导团队成员解决技术难题；确保代码质量和开发进度；负责数据分析与处理，优化 AI 模型训练和反诈策略效果；负责与前端团队的协作。
- 范潇宇：数据架构师 / Neo4j 开发
  - 角色定位： 专注于数据架构和数据库操作，负责知识图谱的构建、维护和优化。
  - 职责： 设计知识图谱模式（Schema）；优化数据存储和查询效率；确保知识图谱能够支撑智能预警和案件分析；负责 Neo4j 数据库的开发与维护。
- 祖少楠：数据工程师
  - 角色定位： 负责反诈所需各类数据的收集、整理、清洗和初步分析。

- 职责： 从新闻、公开案例、报告等渠道收集非结构化信息；进行数据预处理，为知识图谱填充做准备；协助数据架构师进行数据建模。

- 葛世文：用户体验设计师 / 前端开发
  - 角色定位： 负责产品的用户界面设计和前端开发，确保用户体验友好、流畅。
  - 职责： 进行用户界面（UI）和用户体验（UX）设计；负责前端页面的开发与维护，实现响应式设计；与后端团队协作，确保前后端数据交互顺畅。

运营与市场部

- 付宇航：运营总监
  - 角色定位： 负责平台的日常运营、用户增长和社区管理。
  - 职责： 制定运营策略，提升用户活跃度和留存率；管理和维护社区内容，确保社区健康发展；组织线上线下活动，增强用户参与度；负责用户反馈收集与分析。

- 王生斌：市场总监
  - 角色定位： 负责项目的品牌建设、市场推广和商务拓展。
  - 职责： 制定市场营销策略，提升品牌知名度；拓展 B2B/B2G 合作渠道，与金融机构、政府部门等建立合作；负责广告投放和内容传播；进行市场调研和用户需求分析。

- 姜斌：内容策划
  - 角色定位： 负责反诈教育内容的策划、编写和更新。
  - 职责： 策划游戏化学习内容和互动任务；编写反诈科普文章、案例分析等；与技术团队协作，将知识图谱内容转化为用户友好的形式；确保内容的时效性和准确性。

2.4 团队优势与互补性

深厚的技术背景： 团队成员基本都来自计算机相关专业，这为理解和应用前沿技术（如 AI、大数据、图数据库等）奠定了坚实的基础。计算机专业的系统化训练使他们能够运用科学的方法解决复杂的软件工程问题。

丰富的实践经验： 团队拥有多种类应用开发、测试、维护的经验。这意味着他们不仅懂得如何从零开始构建软件，也了解软件生命周期中的各个环节，包括需求分析、设计、编码、测试以及后期的运营和维护。这种全面的实践经验能够为“澄源”项目提供较为成熟和可靠的软件解决方案。

关键技能的互补： 团队成员在项目管理、前后端开发、数据分析和数据库等关键领域各有侧重，形成良好的技能互补。夏雨轩负责顶层设计和项目全局，李发渊主导开发和数据应用，范潇宇深耕数据库基础。这种组合使得团队能够高效地处理项目从概念到实现的各个层面，避免出现明显的短板。

与项目目标的契合： 团队的技术优势（特别是开发和数据分析经验）与“澄源”项目的核心需求（构建知识图谱、应用 AI、处理反诈信息）紧密匹配。他们具备将反诈知识转化为可操作的、智能化的应用能力，这是项目成功的关键保障。

解决复杂问题的能力： 面对电信网络诈骗这种“诈骗手段不断翻新、隐蔽性迷惑性强、黑灰产业链环环相扣”的治理难题，需要团队具备快速学习和解决复杂技术问题的能力。他们的技术背景和实践经验为此提供了基础。

三、问题陈述

3.1 行业背景与现状

在数字化浪潮席卷全球的当下，网络安全已不再是边缘议题，而是事关国家安全、社会稳定以及每个公民切身利益的战略性问题。2024 年是中国全功能接入国际互联网 30 周年，网络空间已深度融入社会生活的方方面面，成为主要的活动载体。随之而来的电信网络诈骗，作为一种以非法占有为目的，利用电信网络技术手段，通过远程、非接触方式诈骗公私财物的行为，其严峻性、复杂性和危害性日益凸显。

以下两图清晰地展示了近年来电信网络诈骗案件数量居高不下的严峻态势：

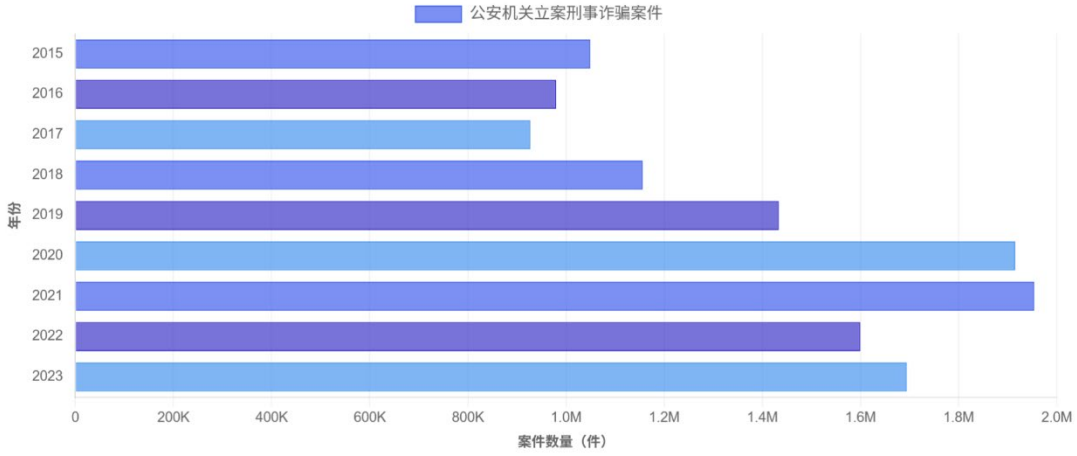

图 3.1-1 公安机关立案刑事诈骗案件 2015-2023 信息来源：国家统计局官网

图 3.1-1 显示，2015 年至 2023 年公安机关立案侦办的刑事诈骗案件数量。从数据中可以看出，尽管每年都有波动，但整体立案数量长期维持在高位：

2015 年至 2018 年，立案数量徘徊在百万件以上。2019 年起，案件数量显著攀升，突破 140 万件。尤为突出的是，2020 年至 2021 年，立案数量激增至近 200 万件，分别高达约 190 万件和 195 万件，表明电信网络诈骗犯罪活动异常猖獗。即使在 2022 年有所回落后，2023 年立案数量又再次上升，超过 170 万件，显示出此类犯罪的顽固性和反复性。

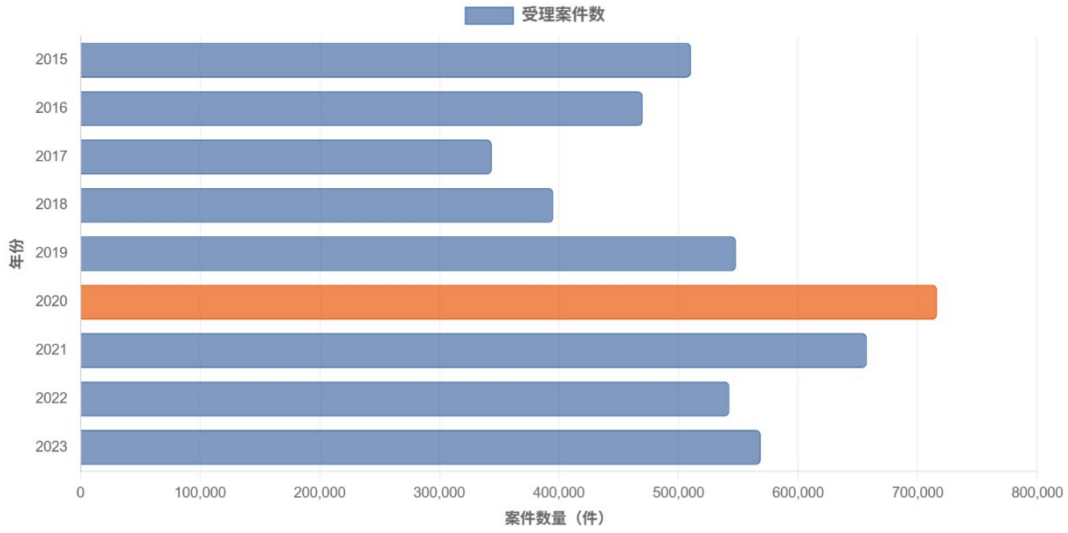

图 3.1-2 公安机关诈骗案件受理数 2015-2023 信息来源：国家统计局官网

图 3.1-2 展示了 2015 年至 2023 年检察机关受理的诈骗案件数量。这一数据同样印证了诈骗案件的高发态势：

检察机关受理的案件数量同样维持在较高水平，尤其在 2020 年达到高峰，超过 70 万件，与同期公安机关立案数量的激增趋势高度吻合。即使在 2021 年之后，受理案件数量也始终保持在 55 万至 65 万件之间，这进一步表明了大量诈骗案件持续进入司法程序。

综合来看，这两组数据共同揭示了当前电信网络诈骗案件数量巨大、持续高发、居高不下的严峻现实。面对如此巨大的案件体量，仅依靠传统的事后打击已难以完全遏制其蔓延。因此，加强事前预防、提升公众反诈意识，已成为刻不容缓的当务之急，也正是反诈应用所能发挥的关键作用。

电信网络诈骗具有显著的特点，图 3.1-1 给出了从作案手法到黑色产业链的全面解析，具体特点如下：一是蔓延性广、发展迅速，能够在短时间内波及大量人群，造成广泛损失。二是诈骗手段快速翻新迭代，犯罪分子不断变化手法，甚至利用恶意程序、诈骗网址、伪基站、AI 换脸等工具作案。在线交易中的虚假评论、虚假宣传、刷单等问题也与电信网络诈骗的本质紧密相连，2024 年的调查显示公众感知到的刷单现象有所攀升。三是形式集团化，反侦查能力强，犯罪团伙分工精细，已形成完整的黑灰产业链，包括引流、话务、技术、洗钱等环节。四

是跨国跨境作案突出，诈骗窝点常设境外，如东南亚、南亚、非洲等地，增加了打击和取证难度。同时，互联网应用的普及伴随着撞库、盗号、薅羊毛、虚假粉丝、洗钱、钓鱼攻击等多种有组织攻击风险。个人敏感信息泄露及其安全问题已成为网民关注的焦点。

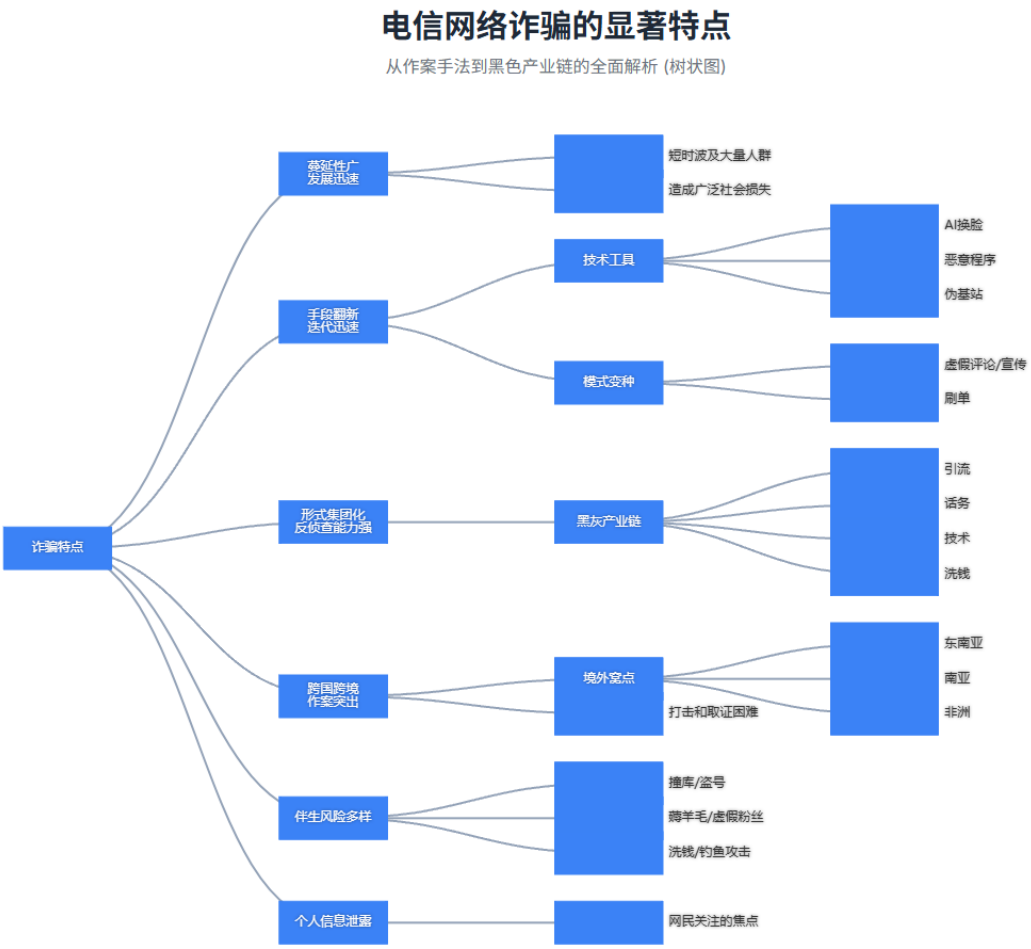

图 3.1-1 电信网络诈骗的显著特点（矩形树图）

电信网络诈骗的受害群体广泛，且骗局往往针对不同人群的特定心理和需求进行“量身定制”。图 3.1-2 给出了电信网络诈骗受害群体与战术分析，不同年龄段的风险不同，18-40 岁人群因网络活动频繁易受网络购物、投资、交友诈骗影响，老年人则易成为健康养老、投资等骗局目标。职业因素也有影响，无业人员、企业财务人员、退休人员等是易受骗群体。高校学生群体也因社会经验相对不足、渴望快速获利、对新兴事物认知有限、易受诱惑而成为主要受害群体。诈骗者通过有限的真实信息建立初步信任，利用虚假信息构造虚幻利益，并利用人

性的弱点，如贪婪、对权威的敬畏、对沉没成本的不甘（“执迷状态”）等，将受害者引入陷阱。信任的建立和维系是诈骗成功的关键。

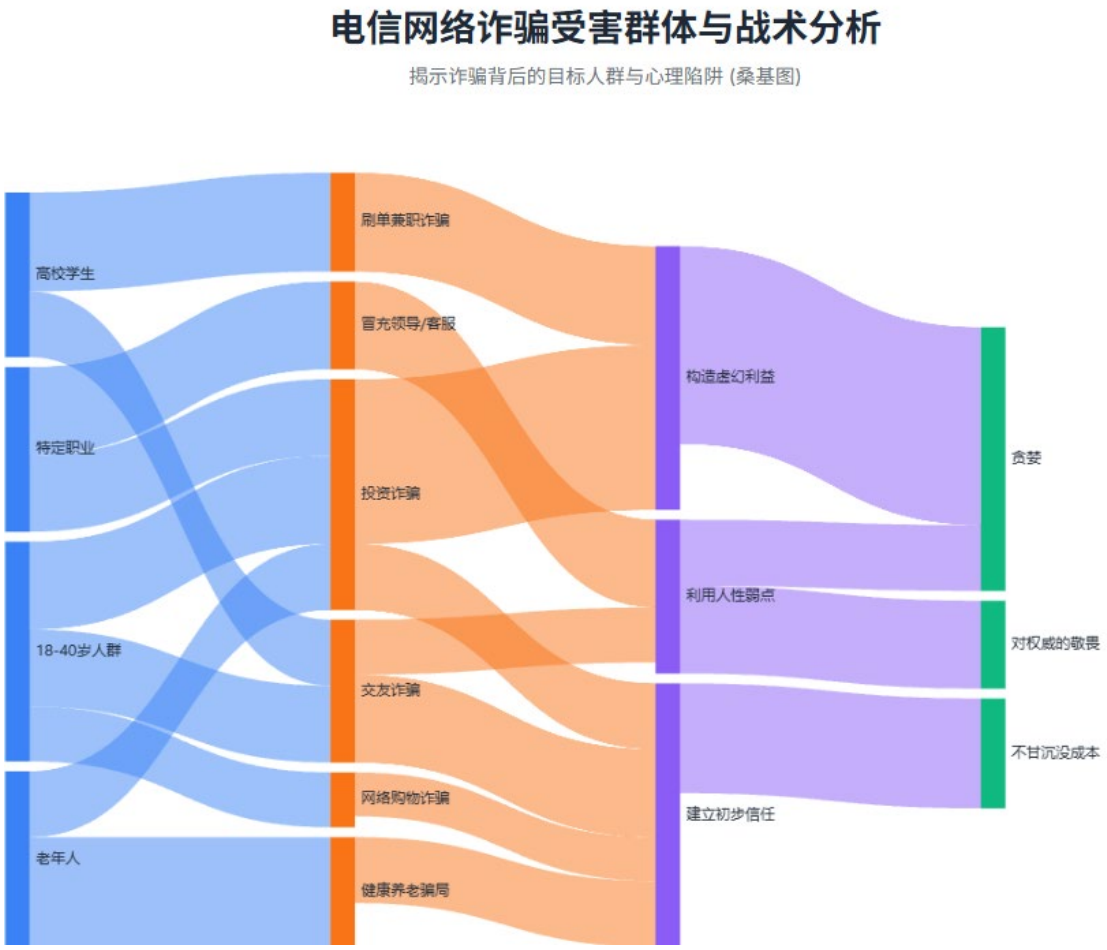

图 3.1-2 电信网络诈骗受害群体与战术分析

为了应对这一日益严峻的挑战，中国政府构建了多层次、全方位的打击治理体系。国务院建立了反电信网络诈骗工作机制，统筹协调全国的打击治理工作。地方各级人民政府组织领导本行政区域内的反诈工作。公安机关牵头负责，金融、电信、网信、市场监管等部门依据各自职责履行监管主体责任。人民法院、人民检察院发挥审判、检察职能作用。

在法律层面，《中华人民共和国反电信网络诈骗法》于 2022 年 12 月 1 日起施行，提供了重要的法律保障。该法确立了“以人民为中心，统筹发展和安全”、“源头治理、综合治理”以及“齐抓共管、群防群治”的原则。这标志着反诈工作从被动打击转向主动预防和全社会共同治理。法律首次在国家层面明确了电信业务

经营者、银行业金融机构、非银行支付机构、互联网服务提供者等相关主体承担风险防控的法定责任，要求其建立内部控制机制、安全责任制度，加强新业务涉诈风险评估。法律在电信治理（如实名制、办卡限制、异常卡监测），金融治理（如客户尽职调查、账户限制、异常交易监测、涉案资金查冻），互联网治理（如服务实名制、异常账号处置、APP 管理、涉诈信息处置）等方面提出了具体要求并规定了法律责任。法律还强调了部门协作、数据共享、技术反制、宣传教育和信用惩戒的重要性。国家鼓励研发反制技术，用于监测识别和封堵涉诈信息活动，并推进网络身份认证公共服务建设。公安机关会同相关部门建立预警劝阻系统，加强追赃挽损。

在法律框架下，各部门和行业也推出了具体措施。公安部协同有关部门推出的“五大反诈利器”是重要组成部分，包括国家反诈中心 APP（累计预警 2.3 亿次），96110 预警劝阻专线，12381 涉诈预警劝阻短信系统，全国移动电话卡“一证通查”服务，云闪付 APP“一键查卡”。金融机构也在技术上积极投入，例如工商银行构建了应用设备指纹、机器学习、知识图谱、智能决策引擎等技术的设备反欺诈系统，在精准识别团伙欺诈和保护被诱导转账受害人方面取得了成效。政策层面也强调加强反电信网络诈骗宣传，普及法律知识，提高公众防骗识骗能力。教育部门、社区等被要求针对老年人、青少年等群体加强宣传教育，“五进”活动便是具体体现。

然而，尽管法律法规逐步健全、技术手段不断升级、政府和行业投入巨大，电信网络诈骗犯罪依然严峻复杂，并且手段不断翻新，这正是我们项目出现的重要原因。

3.2 现有解决方案的局限性

当前的行业背景下，反诈体系在全民宣传教育和主动防御方面仍面临显著挑战：

- 技术对抗的持续升级与隐蔽性： 诈骗技术和黑灰产工具升级速度快，攻防对抗激烈。团伙化、产业化运作使其具有高隐蔽性。传统的风控系统难以检测模拟正常客户行为的复杂欺诈。即使是大型银行，在 ML/DL 技术应用于核心业务反诈方面也存在数据架构、运营解释性等挑战。

- 信息泄露与虚假信息泛滥： 跨领域的信息泄露是诈骗的前提。不法分子利用仿冒 APP、虚假网站等难以完全杜绝，应用市场的审核和监管仍存在乱象，给用户带来风险。

- 公众防范意识与能力不足： 尽管有法律和宣传，但公众特别是部分易受骗群体（如大学生）对反诈宣传漠不关心，心存侥幸，或因媒介素养不足、缺乏洞察力而难以辨别虚假信息。诈骗者利用人性的弱点，如对快速获利的渴望、对权威的信任，以及“登门槛效应”和“拒绝沉没成本心理”，使受害者陷入难以进行理性判断的“执迷状态”。传统的宣传教育形式有时难以触达所有群体或缺乏吸引力，大学校园内的反诈教育也面临通报不及时、主题不集中、传播效率低等问题。

- 用户主动防御策略缺失： 目前的研究和实践更多强调被动应对（如收到预警、事后补救），忽视了用户主动识别和反制诈骗行为的价值和方法。

- 用户维权困境： 网购维权仍面临程序繁琐、成功率低、取证困难、监管处罚力度不足等难点。

图 3.2-1 三款反诈小程序

如图 3.2-1 所示，我们在市场中随机抽取了三款小程序，它们功能各异但皆没有融合现如今爆火的大模型相关技术以及“主动式防御”。尽管也有答题活动与阵营排名等，但无成就系统对于用户来说缺少学习驱动力。

正是在这样的行业背景和现状下，为了弥补现有体系在全民宣传教育深度、用户主动防御能力提升以及实时知识更新等方面的不足，我们的“澄源”反诈平台应运而生。项目直接响应了《反电信网络诈骗法》中关于“加强社会宣传教育防范”、“提高公众对各类电信网络诈骗方式的防骗意识和识骗能力”以及“构建全社会反诈的浓厚氛围”的要求。

通过构建动态更新的反诈知识图谱来应对诈骗手段的快速翻新，利用 AI 模拟实战和“主动防御式反诈”来提供实践训练和提升用户警惕性，克服传统宣传的被动性，通过游戏化和社区生态提升学习兴趣和用户参与度，形成群防群治氛围，我们的项目旨在为公众提供一个创新、高效的反诈学习和实践平台，是对现有反诈体系的有力补充和积极探索。

3.3 痛点分析与量化

公众痛点：

- 信息识别困难： 难以辨别海量网络信息中的虚假内容，难以识别诈骗分子伪装的身份和虚幻的利益诱饵。
- 教育模式不足： 现有反诈宣传和教育可能形式单一，不够生动，难以激发主动学习兴趣，导致防范意识停留在表面。
- 信任陷阱： 容易因诈骗者提供的少量真实信息或小额回报而建立初步信任，进而陷入“执迷状态”，对沉没成本不甘心而持续投入。
- 维权困境： 遭遇诈骗后，维权过程繁琐、耗时，导致许多人放弃维权。
- 个人信息泄露担忧： 网民对个人敏感信息安全高度关注。

行业/机构痛点：

- 技术对抗挑战： 诈骗技术快速迭代，现有技术防范能力面临更高要求。
- 数据整合与分析障碍： 机构内部数据孤岛，难以形成全景视图进行有效的风险监测和分析。
- 运营效率低下： 传统风控运营依赖复杂流程和跨部门协调，效率不高。
- 信息共享不足： 监管部门、金融机构、电信运营商、互联网服务提供者之间的信息共享和协同不足。

量化：

- 2024 年网购安全调查收到专题问卷 116,996 份，反映公众高度关注。
- 刷单现象依然普遍存在，超三分之二受访者感知到。

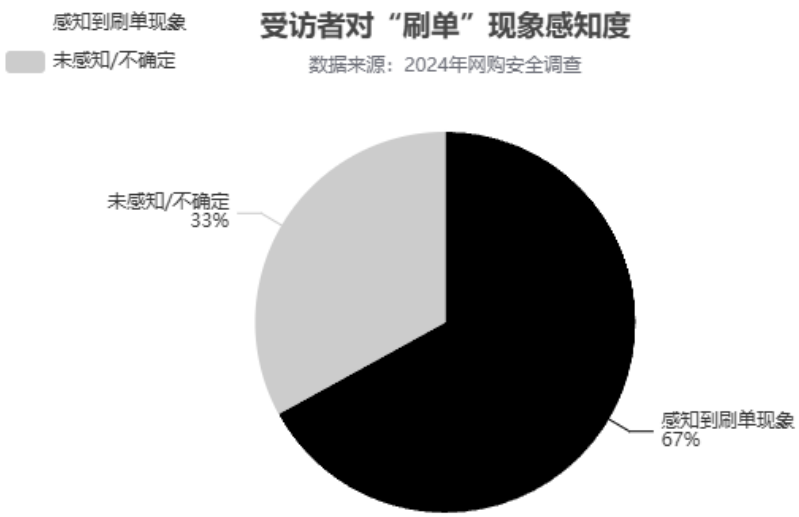

图 3.3-1 受访者对“刷单”现象感知度

- 2022-2024 年，全国各级法院一审审结电信网络诈骗犯罪共计 3095 件。
- 国家反诈中心 APP 累计预警 2.3 亿次，仍需进一步防范。

四、项目内容

4.1 产品/服务概述

面对日益猖獗且快速变化的电信网络诈骗，以及传统宣传教育模式吸引力不足的挑战，“澄源”作为一款创新的智能反诈演练平台应运而生。为了方便用户随时随地进行学习，我们的服务将通过易于访问的 Web 页面和专属移动 App 提供，确保您能在任何设备上获得无缝的反诈体验。平台通过结合以下核心功能，致力于帮助用户在沉浸式的互动体验中轻松掌握反诈技能，弥补现有解决方案在用户参与度和教育有效性上的短板，从而有效提升全民防范意识与能力：

- 诈骗关系网： 将复杂的诈骗手法、人物关系、资金流向等信息以直观的图形化方式呈现，帮助用户快速理解诈骗的本质和套路，洞悉诈骗团伙的运作模式。
- AI 模拟诈骗实战： 利用人工智能技术，模拟真实的诈骗场景和对话，让用户亲身体验各类诈骗陷阱，在安全的环境中提升识别和应对诈骗的能力。
- 创新的“主动防御”模式： 不仅提供事后补救，更侧重于事前预警。通过分析用户行为模式、接收到的信息等，提前识别潜在风险，并及时发出预警和防范建议，变被动为主动。
- 游戏化学习社区： 将反诈知识融入趣味性游戏和互动任务中，通过积分、排名、成就等机制激发用户学习兴趣，并在社区中分享经验、交流心得，共同提升反诈技能。

“澄源”通过这些创新功能，旨在打造一个全方位、多维度、高参与度的反诈学习平台，让用户在寓教于乐中真正掌握防骗技能，筑牢个人和家庭的反诈防线。

图 4.1-1 成果物展示

“澄源”的核心技术架构以构建并持续维护强大的反诈知识图谱为基石。该知识图谱采用高性能、灵活扩展的 Neo4j 图数据库作为底层支撑，能够有效存储和高效查询复杂的诈骗网络关系。在知识获取层面，“澄源”创新性地融合了先进的自然语言处理（NLP）技术 或通过微调大语言模型（LLM），实现对海量非结构化反诈相关信息（如每日新闻热点、公开诈骗案例、反诈研究报告等）的智能、自动化抽取。这包括高效识别并抽取诈骗手段、诈骗团伙（角色、组织结构）、受害者特征、资金流向、常用诈骗话术、利用的人性弱点及骗术类型等关键实体与复杂关系，并将这些信息结构化、规范化地存储于知识图谱中，确保反诈知识体系的实时更新与动态演进。知识图谱的应用有助于通过提供额外上下文信息来增强 AI 模型性能，改善对自然语言的理解，并通过结构化信息源帮助创建更具交互性和智能的 AI 系统。

基于功能强大的知识图谱和 AI 技术核心，“澄源”平台提供以下关键功能和服务：

- 诈骗关系网：为用户提供知识图谱的可视化界面，帮助用户直观理解诈骗网络、关联方以及诈骗手法的内在联系，从而增强对复杂诈骗模式的认知。
- AI 模拟诈骗实战：用户可以随时与模拟“骗子”的 AI 进行对话，体验各种类型的诈骗场景，例如网络贷款、刷单返利、“杀猪盘”、冒充电商物流客服等常见骗局。系统会根据用户的应对实时反馈诈骗进展，并在结束后进行专业

分析，指出用户在识别过程中的漏洞，提供有针对性的实战训练和反馈。这种模拟有助于提升用户在真实情境下的识别和应对能力。

- “主动防御式反诈”：这是一项旨在从心理层面持续激发用户最高级别警惕性的创新性功能。用户在明确知情并自愿选择加入后，将不定期收到精心设计的模拟诈骗信息（如短信、邮件），其中可能包含无害链接。用户点击链接后，应用会立即弹出提醒“你被骗了”，同时明确告知该链接不会获取或损害任何个人数据。此功能的核心在于让用户形成“所有可疑信息都是考验”的思维模式，从而在面对真实诈骗时保持高度警惕和主动防御意识。项目承诺在任何环节不获取、不保存任何用户敏感数据，并提供完备透明的隐私协议。

- 游戏化学习体验：深度融合答题闯关和成就系统，提升学习的趣味性和吸引力。反诈知识点被设计成不同的关卡，用户通过答题闯关积累经验，达成特定学习成就后可解锁更高难度挑战。这种设计旨在激励用户主动学习和巩固反诈知识。此外，学习成就（如“反诈达人”、“火眼金睛”）可分享至社交平台，激发朋友、同学的挑战欲，形成积极的反诈学习社群。游戏化已被证明能有效提高学习者参与度、动机和知识保留率。

- 反诈社区生态：建立一个活跃、互助的反诈信息协作平台。通过智能机器人自动聚合每日诈骗热点新闻、典型案例分析并进行反诈科普。社区设有严格的信息审核机制，并引入专家引导和用户激励机制（优质内容奖励、互动积分等），鼓励用户分享受骗经验、防范知识，并获取权威咨询。

尽管核心反诈功能对所有个人用户免费开放，“澄源”通过以下模式实现可持续发展：

- 定制化解决方案：与金融机构、大型企业及政府部门等机构建立合作，为其提供基于知识图谱和 AI 技术的定制化反诈培训课程、内部风险预警系统、员工反诈能力评估工具及专业数据分析报告等服务。反诈产品在银行、电信运营商、政府部门等领域有应用需求。

- 精选广告投放：严格筛选少量、高品质、内容相关且不干扰用户体验的广告（如反诈安全产品、正规金融服务）作为补充收入来源。

- 项目的核心优势在于其创新性的“主动防御式反诈”理念和 AI 模拟诈骗的实战性结合，能够从心理和实践层面有效提升用户防御能力。高度游戏化和社交化的学习互动设计提升用户粘性与参与度。知识图谱、Neo4j 与大模型的深度融合构建了强大的智能核心，形成技术壁垒。项目目前已完成原型开发和 Demo，具备初步功能验证能力，展现出快速市场验证与迭代潜力。

“澄源”不仅是一款技术驱动的反诈工具，更致力于成为一个赋能全民、共建安全数字社会的智能平台。这与国家层面推动“全民反诈、全社会反诈”的氛围相契合。通过将前沿 AI 技术与创新的用户互动模式相结合，“澄源”有潜力有效提升社会整体的反诈能力与意识，为构建更加和谐、安全的数字生活环境贡献力量。

4.2 核心技术架构

“澄源”反诈应用的技术核心在于整合前沿的人工智能、图数据库和用户互动技术，构建一个智能、动态的反诈知识体系和用户赋能平台。以下是其主要技术/组件的详细说明：

知识图谱 (KG)

- 概述与作用： 知识图谱是“澄源”的核心技术基石，用于构建并持续维护一个强大的反诈知识体系。它将海量非结构化反诈信息转化为结构化的知识表示，以实体（节点）和关系（边）的形式存储，能够有效组织、整合多源异构的威胁数据。

- 底层技术： 项目采用高性能、灵活扩展的 Neo4j 图数据库作为知识图谱的底层支撑。Neo4j 是一种原生图数据库，广泛应用于知识图谱、欺诈检测等领域。它能够高效存储和查询复杂的诈骗网络关系，例如诈骗手段、团伙结构、资金流向、常用话术、利用的人性弱点等关键实体及其相互关联。

- 构建流程： 知识图谱的构建涉及信息提取、增强、扩展和迭代细化等阶段。这要求精确的信息抽取技术，特别是实体识别和关系抽取。

- 数据来源与更新：知识图谱的数据来源于对每日新闻热点、公开诈骗案例、反诈研究报告等多源异构数据的实时抓取与深度分析。通过智能、自动化抽取关键实体与复杂关系，确保反诈知识体系的实时更新与动态演进。构建过程可能需要定义清晰的图谱模式，包括允许的节点和关系类型，以提高提取的一致性和准确性。

- 技术优势： 基于知识图谱的应用有助于通过提供额外上下文信息来增强 AI 模型性能，改善对自然语言的理解，并通过结构化信息源帮助创建更具交互性和智能的 AI 系统。它能帮助用户直观理解诈骗网络、关联方及其内在联系。

人工智能 (AI) 与机器学习 (ML)

- 概述与作用： AI 和 ML 技术贯穿于“澄源”的多个核心功能，为反诈工作提供多维度、深层次的赋能。AI 在安全教育培训领域的应用前景广阔，能提供个性化、互动性强的培训体验。

- 关键应用：

  - AI 模拟诈骗实战： 利用 AI 技术，特别是大型语言模型的强大生成能力，扮演高度拟真的“骗子”角色，生成具有真实场景感的多轮诈骗对话，为用户提供沉浸式实战对抗体验。这有助于提升用户在真实情境下的识别和应对能力。

  - 个性化知识服务与智能咨询： 结合知识图谱的结构化优势与 AI 的自然语言理解能力，为用户提供精准、个性化的反诈咨询与建议，并辅助生成反诈科普内容。

  - 智能信息抽取与分析： 利用 AI/ML 技术（结合 NLP/LLM）实现对海量非结构化反诈信息的智能、自动化抽取与分析，为知识图谱的构建和更新提供数据。

- 风险识别与模式挖掘： 在模拟诈骗中分析用户的应对，识别其识别漏洞。在潜在的机构合作场景下，AI 与知识图谱结合，可用于识别团伙犯罪的关联性并挖掘潜在欺诈风险。

- 新兴趋势： 近年来，AI 技术（如 AI 换脸、语音合成）也被诈骗分子利用，增加了诈骗的隐蔽性和防范难度。反诈领域的技术攻防对抗日趋激烈，对技术防范能力提出更高要求。

自然语言处理 (NLP)

- 概述与作用： NLP 是实现从非结构化文本中提取信息以构建知识图谱的关键技术之一。

- 应用： “澄源”利用 NLP 技术实现对每日新闻热点、公开诈骗案例、反诈研究报告等非结构化数据的智能、自动化抽取，识别并抽取诈骗手段、团伙、受害者特征等关键实体与关系。实体识别和关系抽取是 NLP 在知识图谱构建中的核心任务。

大型语言模型 (LLM)

- 概述与作用： 大型语言模型在人工智能领域取得了爆发式发展，其强大的生成、理解与分析能力为“澄源”提供了重要的技术支撑。

- 应用：

  - 信息抽取： 通过微调 LLM 或利用 LLM 图转换器，提高从反诈相关文本中抽取实体和关系的效率和准确性。

  - AI 模拟诈骗： LLM 是驱动 AI 模拟诈骗对话的核心，根据知识图谱生成高度拟真的诈骗场景和对话。这属于利用 AI 进行沉浸式安全操作模拟训练的一种形式。

  - 内容生成： 辅助生成权威、通俗易懂的反诈科普内容。

  - 智能代理： LLMs 可以驱动智能代理，根据上下文决定是直接回答问题还是调用工具（如知识图谱查询）来获取信息。

- 集成： LLMs 可以与 LangChain 等框架以及 Neo4j 图数据库结合使用，构建知识图谱并增强检索生成（RAG）应用。 LLMs 支持结构化输出和函数调用，有助于提高 KG 构建效率和 Agent 的决策能力。

行为分析/模式识别

- 概述与作用： 行为分析和模式识别用于理解和预测用户的行为，以及识别潜在的欺诈模式。
- 应用：
  - 用户薄弱环节识别： 在 AI 模拟诈骗实战中，系统分析用户应对过程中的反应，识别其在反诈识别和应对能力方面的薄弱环节。
  - 欺诈模式挖掘： 结合知识图谱和 AI 技术，分析海量数据，识别欺诈团伙的关联性及行为模式。这与银行反诈系统中利用设备指纹、风险画像和知识图谱挖掘团伙欺诈类似。行为分布特征是欺诈风险管理的重要指标。
  - 风险预警： 分析潜在受害者的行为模式，及时发现并采取劝阻措施。

游戏化引擎

- 概述与作用： 游戏化引擎用于将游戏元素和游戏设计技术应用于非游戏环境（如学习和培训）中，以提高用户的参与度、动机和学习效果。
- 应用： “澄源”通过深度融合答题闯关和成就系统来提升反诈学习的趣味性和吸引力。
- 功能： 实现知识点关卡设计、答题闯关、经验积累、成就解锁（如“反诈达人”、“火眼金睛”）。
- 效果： 游戏化已被证明能有效提高学习者参与度、动机和知识保留率。分享学习成就至社交平台可激发社交互动和学习氛围。

技术组件

- 概述与作用： 社区平台提供用户交流、互助和信息协作的空间。
- 功能： 支持用户分享受骗经验、防范知识、获取权威咨询。通过智能机器人自动聚合每日诈骗热点新闻、典型案例并进行反诈科普。具备严格的信息审核机制，并引入专家引导和用户激励机制（如优质内容奖励、互动积分）。建立活跃、互助的反诈信息协作平台符合共建反诈的社会氛围。

数据分析与可视化

- 概述与作用： 数据分析用于收集、处理和解释用户行为、学习进度和平台互动数据，以评估产品效果、优化功能和为机构客户提供报告。可视化则用于直观展示复杂信息。
- 应用：
  - 知识图谱可视化： 利用可视化工具（如项目中提到的 ECharts）向用户展示知识图谱结构，帮助用户直观理解诈骗网络和关联信息。图可视化是 Neo4j 生态系统的一部分。
  - 用户行为分析： 分析用户在 AI 模拟、游戏化闯关、社区互动中的行为数据，评估学习效果和参与度。
  - 机构报告： 为合作的金融机构、企业及政府部门提供专业的反诈能力评估工具及专业数据分析报告。
  - 趋势分析： 结合知识图谱和数据分析，识别诈骗手法、受害者特征等的分布特征和趋势。

技术栈：

- 后端服务：项目采用成熟且可扩展的 Django 技术栈构建后端，负责核心业务逻辑、数据接口（API）开发及与 Neo4j 图数据库的交互。

- 前端界面： 采用用户体验友好的 Nuxt。js 框架开发前端界面，实现响应式设计。
- 数据库： 使用 Neo4j 图数据库存储知识图谱。
- 发展阶段：项目目前已完成原型开发并制作出 Demo，具备初步功能验证能力，展现出快速市场验证与迭代潜力。

综上所述，“澄源”在技术上围绕反诈知识图谱构建了一个智能化的应用层，通过 AI 赋能实战模拟和个性化服务，通过游戏化和社区建设增强用户粘性，并利用数据分析和可视化提升用户认知和产品洞察。其技术架构和功能设计充分考虑了当前电信网络诈骗的特点和反诈工作的需求，与国家层面推动“全民反诈”的氛围相契合。

4.3 核心功能模块详解

诈骗关系网： 用户可以直观地探索不同诈骗类型、手法、关联因素之间的联系。 知识点结构化呈现，帮助用户理解复杂信息。

AI 模拟诈骗实战： 用户与 AI 扮演的“骗子”进行对话练习，体验多种诈骗场景。 系统实时反馈，结束后提供专业分析，指出用户应对漏洞。

主动防御式反诈： 用户自愿订阅后，不定期接收模拟诈骗信息（短信、邮件等），点击无害链接后立即提示“你被骗了”。 旨在强化“所有可疑信息都可能是考验”的思维模式。 承诺不获取、不保存用户敏感数据。

反诈社区生态： 智能机器人自动聚合热点新闻、典型案例、科普知识。 用户分享受骗经验、防范知识。 严格审核机制，专家引导，用户激励。

游戏化学习体验： 基于知识图谱的“反诈知识库”，将知识点设计成关卡，用户通过答题闯关积累经验，解锁成就。 成就可在社区内分享，激发学习积极性。

以下是产品的低保真原型图（包含 web 端与移动端）

Web 端：

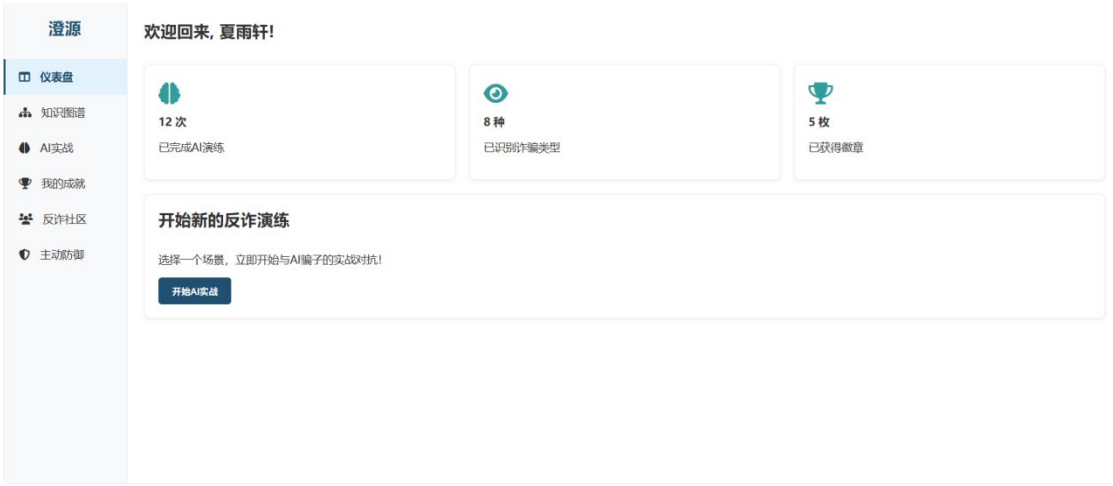

图 4.3-1 仪表盘

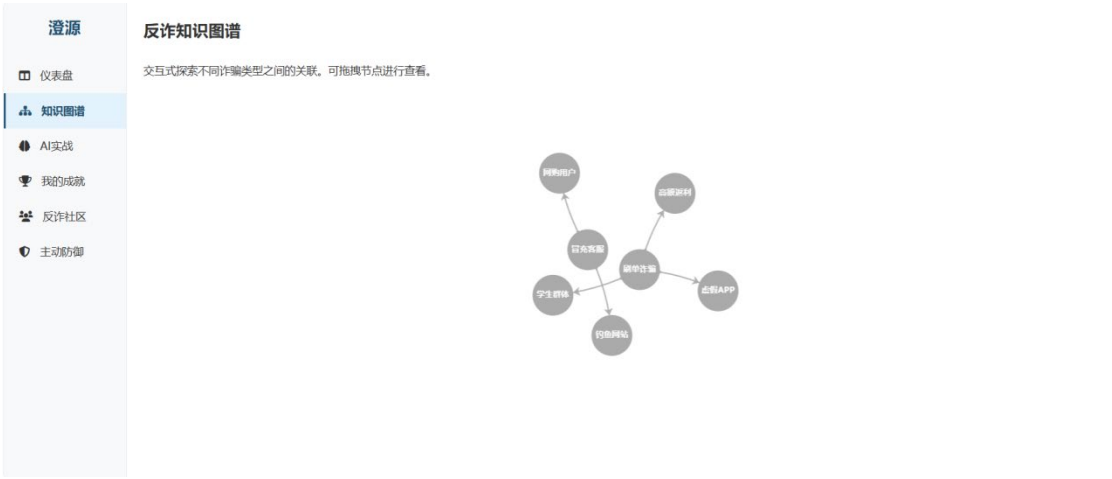

图 4.3-2 知识图谱

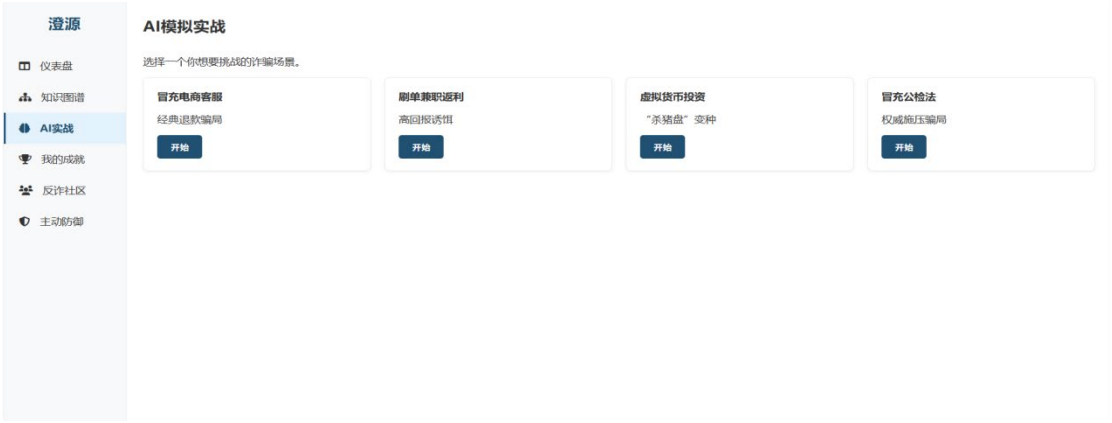

图 4.3-3 AI 实战

图 4.3-4 我的成就

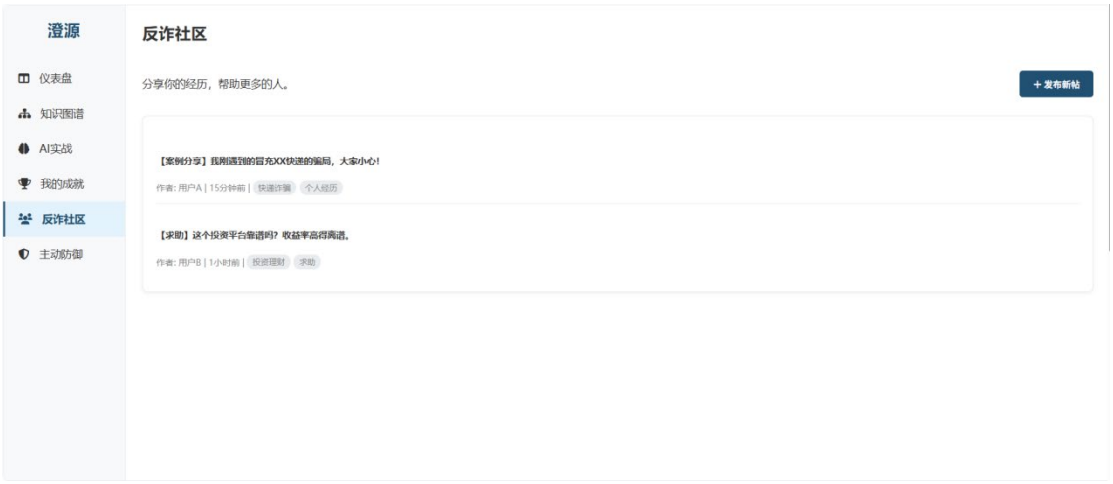

图 4.3-5 反诈社区

图 4.3-6 主动防御

移动端：

图 4.3-7~8 UI 界面

4.4 产品路线图

我们的“澄源”项目旨在构建一个创新、高效、用户友好的基于知识图谱与大模型的反诈新范式，打破传统反诈宣传的局限性，通过技术赋能和模式创新，提升公众尤其是高校学生的反诈意识和主动防御能力。基于当前行业背景下反诈体系在全民宣传教育深度、用户主动防御能力以及实时知识更新等方面的不足，我们规划了以下阶段性的产品路线图，以逐步实现项目愿景：

第一阶段 (MVP)：构建智能反诈基石与核心功能验证

本阶段的核心目标是快速构建项目的基础技术框架和核心功能模块，并进行初步的用户获取和体验验证，确保项目方向的可行性。我们将专注于：

- 构建基础反诈知识图谱： 利用 Neo4j 图数据库 存储反诈知识，从公开渠道（如新闻报道、反诈案例、研究报告）初步抽取关键实体（如诈骗类型、手法、目标群体、作案工具、地理位置）及其关系。此阶段的知识图谱将是反诈体系智能化的基础，通过结构化数据为后续功能提供支持。

- 实现核心可视化功能： 开发基于 ECharts 的可视化界面，允许用户直观地查阅部分知识图谱，初步了解诈骗的复杂网络和不同骗术之间的关联。这有助于用户摆脱碎片化信息的困扰，形成更系统的认知。

- 开发典型诈骗场景的 AI 模拟实战模块（1-2 个）： 利用大语言模型（LLM）模拟“骗子”角色，基于知识图谱中的典型诈骗剧本（例如，冒充电商客服退款诈骗、刷单返利诈骗等高发类型），生成具有真实感的多轮对话，为用户提供安全环境下的实战演练机会。这直接回应了现有教育模式缺乏实践训练的问题。

- 搭建社区基础功能： 实现用户注册、内容发布（文章、案例分享）、评论、点赞等基本互动功能。引入智能机器人，自动聚合和推送反诈热点资讯和科普内容。构建社区旨在促进信息共享和用户互助，营造群防群治氛围。

- 实现简单的游戏化机制： 引入基础的积分系统，用户通过完成学习任务、参与社区互动等获取积分。 设置简单的成就（例如，完成首次模拟实战），提升用户参与的趣味性。

- 专注于核心用户获取和基础体验验证： 优先面向高校学生群体推广，收集用户反馈，快速迭代优化核心功能和用户体验。

第二阶段：扩展内容深度，增强互动与防御能力

在 MVP 稳定运行并获得初步用户反馈后，我们将重点扩展知识内容，增强平台的互动性和创新防御功能：

- 扩展知识图谱内容： 深入集成更多诈骗类型、变种手法（如 AI 换脸、新型蟹卡、FaceTime 诈骗等）、犯罪团伙结构、资金流向等更细致的信息。通过融合自然语言处理技术或微调 LLM，提升从多源异构数据中自动化抽取和更新知识图谱的能力。

- 增加更多 AI 模拟诈骗场景和复杂性： 开发更多样化的模拟实战场景，覆盖不同类型的诈骗手法和针对性人群。 增加对话轮次和复杂度，模拟更狡猾

的诈骗分子话术和心理操纵过程（如利用登门槛效应、沉没成本心理等），提高实战训练的逼真度。

- 完善社区功能，引入专家互动： 邀请反诈专家、心理学专家等入驻社区，提供专业咨询和案例解读。 建立用户激励体系，鼓励用户分享真实受骗经历和防范心得，形成互助学习氛围。 引入严格的内容审核机制，确保社区信息准确性。

- 正式推出“主动防御式反诈”功能（用户选择加入）： 落地项目核心创新点——通过精心设计的模拟诈骗信息推送，在用户知情并自愿的前提下，持续激发其警惕性，训练用户主动识别和反制诈骗行为的能力。 严格遵守用户隐私承诺。

- 完善游戏化学习体验： 将知识图谱中的知识点体系化，设计成答题闯关、升级、解锁成就等游戏化流程。 增加社交分享属性，鼓励用户展示成就、邀请好友参与，扩大平台影响力。

第三阶段及以后：深化技术集成，拓展平台边界与影响力

- 进入成熟发展阶段，我们将进一步深化技术应用，探索商业模式，并扩大平台的覆盖范围和影响力：

- 深度集成 LLM 能力： 将 LLM 更紧密地集成到知识图谱的构建流程中，利用其强大的文本生成和理解能力，实现更智能、更高效的信息抽取、知识整合和动态更新。 同时，利用 LLM 优化 AI 模拟实战的对话逻辑和逼真度。

- 探索 B2B/B2G 服务模式的商业化落地： 基于已构建的强大知识图谱和 AI 能力，为金融机构（如银行）、大型企业、政府部门 等提供定制化反诈培训解决方案、内部风险识别辅助工具、员工反诈能力评估和专业数据分析报告等服务。 这将是项目重要的盈利来源，支撑持续发展。

- 开发定制化模块： 针对特定易受骗群体或高风险人群，开发有针对性的反诈知识内容和模拟场景。 例如，为老年人设计更易理解、贴近其生活场景的防骗课程（如养老投资、保健品诈骗）；为学生定制校园贷、网络游戏交易、

兼职刷单等骗局的深度剖析和模拟；为金融从业者提供行业相关的欺诈风险培训。

- 优化用户体验，增加跨平台支持： 在现有 Web 端的基础上，我们将积极拓展移动端应用。一个重要的里程碑将是推出“澄源”安卓 App 版本。 考虑到中国广大网民特别是学生群体对移动应用的重度依赖，以及安卓系统在国内的普及度，开发原生的安卓 App 能够极大地提升用户体验，提供更流畅的交互、更及时的预警通知以及更便捷的访问方式。虽然当前市场存在官方反诈 App，但部分用户对其安装方式和隐私权限存在疑虑。我们的安卓 App 将坚持自愿下载、透明权限和严格隐私保护原则，为用户提供一个安心可靠的移动反诈学习和实践平台。后续也可能考虑 iOS 或其他平台的应用开发，以覆盖更广泛的用户群体。技术上，我们将利用现有的后端 API 接口，结合安卓原生开发语言（如 Java 或 Kotlin），实现移动端的各项功能。

- 持续迭代，应对新的诈骗手段： 电信网络诈骗犯罪手段迭代迅速。我们将建立常态化的威胁情报收集和分析机制，持续更新知识图谱，并快速将最新的诈骗手法融入到 AI 模拟实战和教育内容中，确保平台信息的时效性和有效性。

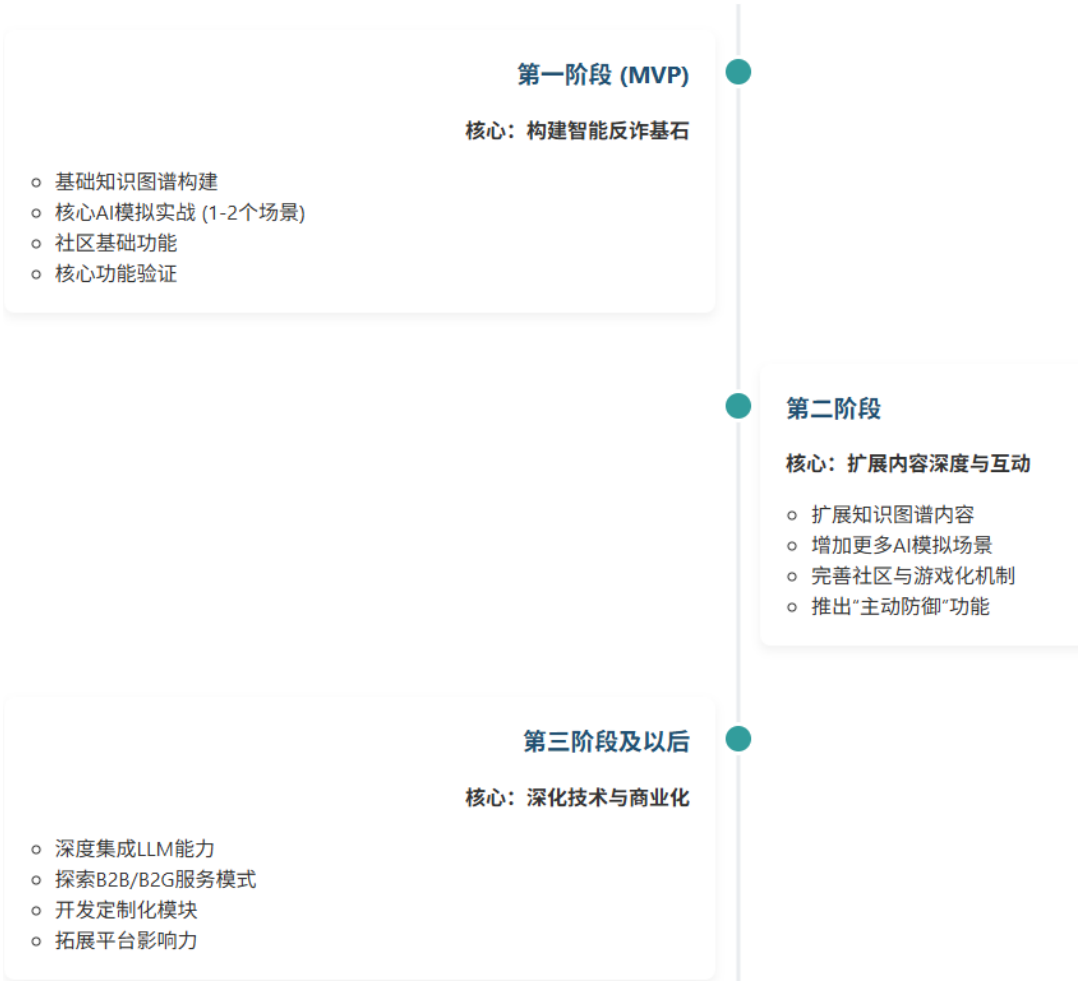

图 4.4-1 澄源产品路线图

通过以上分阶段的产品路线图，“澄源”将从一个基础的反诈平台逐步成长为一个集智能学习、实战演练、社区互动和专业服务于一体的立体化反诈体系，最终目标是成为全民信赖的反诈“防火墙”和主动防御的“训练营”。

五、市场分析

5.1 目标市场定义与细分

主要目标市场为广大互联网用户。 重点关注容易成为电信网络诈骗受害者的群体：包括对网络信息信任度较高且社会经验相对不足的年轻人（如大学生、10-29 岁网民占比高）；经济来源不稳定或急于求财者（如无业人员、待业群体）；接触新事物有限的老年人；以及频繁进行网络交易或使用网络办公的人员（如网购群体、企事业单位财务人员）。

市场细分可以根据年龄、职业、上网习惯、易受骗类型等进行：

- 年龄段： 10-19 岁, 20-29 岁 (高占比)；老年人 (易受骗群体)。
- 职业： 学生, 无业/待业, 企业员工 (特别是财务), 退休人员。
- 上网行为：频繁网购者, 直播购物用户, 网络游戏玩家, 社交平台活跃用户。
- 受骗倾向： 容易相信网络交友、投资理财、兼职信息、仿冒身份等的用户。

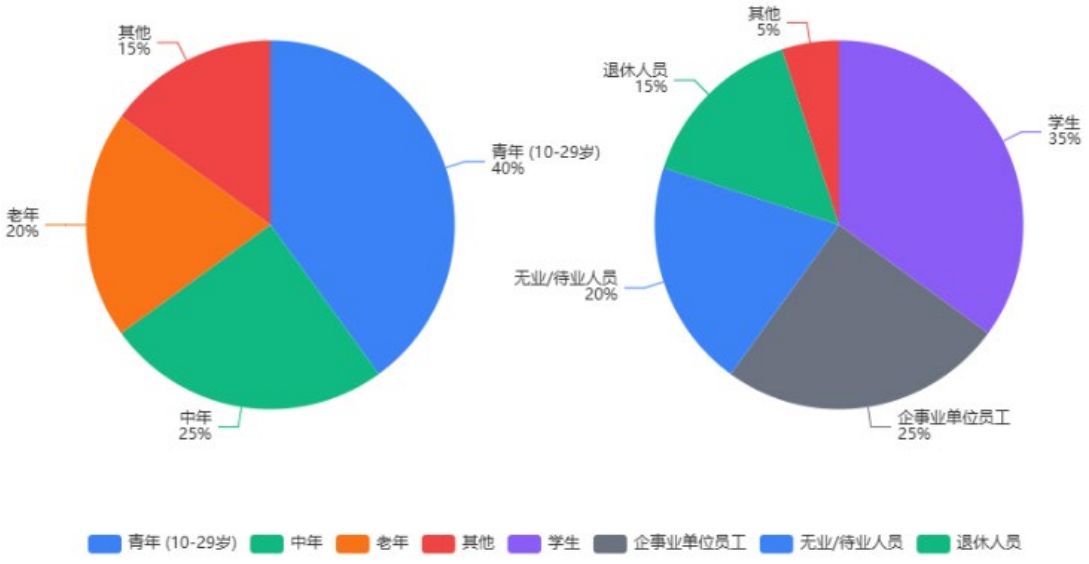

图 5.1-1 目标市场构成分析

5.2 市场规模与增长趋势

中国网民基数庞大。2024 年网民调查活动覆盖全国 34 个省级行政区及部分海外地区。 互联网普及带动了网络经济和线上交易的迅速增长，反诈产品市场也随之增长。 预计全球反诈产品市场规模到 2029 年将达到可观水平。 诈骗手段的不断升级和新场景出现（如直播带货中的问题）持续催生反诈需求。

图 5.2-1 3-5 年市场情况

5.3 行业趋势与发展机遇

政策驱动：

国家对电信网络诈骗问题的高度重视，已转化为系统性的法律法规体系和强有力的监管措施，这为反诈产品和服务的创新与发展奠定了坚实的政策基础和广阔的市场空间。

首先，2022 年 9 月通过并于同年 12 月 1 日起施行的《中华人民共和国反电信网络诈骗法》 是国家打击治理电信网络诈骗工作的关键里程碑。该法明确了电信网络诈骗的概念，强调反诈工作必须坚持“以人民为中心”，统筹发展和安全，并突出“打防结合、防范为先” 的原则，要求加强社会宣传教育防范。法律体系的完善不仅提升了反诈工作的法治化水平，更明确了各方主体责任，包括公安机关牵头，金融、电信、网信、市场监管等部门依照职责履行监管主体责任，以及电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任。这从法律层面要求相关行业必须加强自身反诈能力建设，为本项目面向 B 端（企业/金融机构）和 G 端（政府部门）提供定制化服务创造了直接需

求和合规驱动。法律还明确，有关部门和单位、个人应当对在反电信网络诈骗工作过程中知悉的个人隐私、个人信息予以保密。

其次，高层战略文件提供了行动纲领。中共中央办公厅、国务院办公厅印发的《关于加强打击治理电信网络诈骗违法犯罪工作的意见》进一步强调要构建严密防范体系，强化技术反制，加强预警劝阻，并建立全方位、广覆盖的反诈宣传教育体系，特别指出要开展防范电信网络诈骗犯罪知识进社区、进农村、进家庭、进学校、进企业活动（“五进”活动），形成全社会反诈的浓厚氛围。这与本项目通过平台提供知识普及、实战演练和社区互动来提升公众防范意识的目标高度契合。

再次，国家和相关部门推出了系列具体措施，构筑反诈“防火墙”。这包括“五大反诈利器”：国家反诈中心 APP（累计预警 2。3 亿次）、96110 预警劝阻专线、12381 涉诈预警劝阻短信系统（利用大数据、AI 分析识别潜在受骗用户）、全国移动电话卡“一证通查”服务、云闪付 APP“一键查卡”。这些措施提升了国家层面的预警和防范能力，但也暴露出在用户主动参与和教育方式创新上的不足，为本项目提供了差异化发展的切入点。此外，国家还定期组织“全民反诈在行动”集中宣传月活动，进一步加强反诈宣传力度，提升群众防骗识骗能力。

最后，监管部门加大了对互联网平台乱象的治理力度。例如，工业和信息化部曝光了一批涉诈高风险 App，包括冒用“国家”旗号的虚假 App，显示出 App 市场存在乱象，需要加强监管审核。法律规定，为应用程序提供分发服务的，应当登记并核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途。这些监管要求促使平台方需要更有效地识别和管理风险，对提供风险识别和管理技术的产品形成需求。国家也支持电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者研究开发有关电信网络诈骗反制技术，并利用大数据和人工智能技术进行监测识别和打击，例如工商银行已实践基于设备指纹和知识图谱的反欺诈系统。

这些政策和措施共同构建了一个多层次、全方位的反诈治理格局，不仅提高了全社会的风险意识，也为本项目提出的智能反诈知识平台提供了政策支持和市

场需求驱动，特别是在面向政府和企业提供定制化服务以及加强公众教育方面，政策导向与项目目标高度契合。

技术应用深化： AI、大数据、知识图谱等前沿技术在反诈领域的应用不断深入，从被动打击向主动预防转变。

跨领域协同： 推动政府、社会组织、企业等部门间的协同合作和信息共享。本项目作为连接公众教育和技术能力的平台，有机会与这些部门建立合作。

用户需求升级： 用户不再满足于简单的信息灌输，需要更互动、更个性化、更有趣的学习方式。

细分市场机会： 在金融反诈、电信反诈等传统领域之外，新兴的网络行为（如直播购物）和诈骗类型（如杀猪盘、虚假投资理财）提供了新的防范需求和产品机会。

5.4 目标用户画像与需求分析

以大学生群体为例：

- 人口统计学特征： 18-25 岁左右，通常未经济独立，依赖家庭资助。
- 网络行为： 频繁使用社交媒体、网购、参与网络兼职、网络游戏等。
- 心理需求与弱点： 对金钱有需求，容易被“轻松赚钱”、“高额利润”等虚幻利益诱惑。 信任度相对较高，容易受到虚假信息和社交工程的影响。 容易陷入“执迷状态”，不甘心沉没成本。
- 反诈教育需求： 需要了解最新、常见的诈骗手法。 需要提升识别虚假信息和利益的能力。 需要掌握应对技巧，尤其是在高压或诱惑情境下。 希望反诈学习不枯燥，能互动、有趣、有成就感。

其他用户群体的需求类似，但侧重点不同（如老年人对冒充公检法、养老投资更需警惕；财务人员对冒充领导更需警惕）。

六、竞争分析

6.1 现有竞争者概览

政府官方平台： 国家反诈中心 APP 及其配套服务（预警电话、短信、一键查卡等）。

金融机构内部系统： 各银行、支付机构的反欺诈和风险控制系统。

传统安全/反欺诈公司： 提供 B2B/B2G 服务的技术公司，如同盾科技、亚信科技、腾讯安全天御、百融云创、浙江邦盛科技、阿里巴巴等。

教育机构与社区组织： 开展线下或线上反诈宣传和讲座。

其他潜在竞争者：提供网络安全知识普及、安全教育的平台或内容创作者。

6.2 竞品 SWOT 分析

政府官方平台 (以国家反诈中心 APP 为例)：

- 优势 (Strength)： 国家背书，权威性高；触达广泛，用户基数潜力大；具备直接预警和干预能力（如拦截、止付）。
- 劣势 (Weakness)： 可能面临公众对隐私的担忧；用户主动学习和持续参与的动力可能不足；教育方式可能偏传统，缺乏互动性和趣味性。
- 机会 (Opportunity)： 政策支持，推广力度大；可与本项目合作，形成互补。
- 威胁 (Threat)： 如果本项目无法与其形成明显差异化，可能难以吸引用户。

金融机构内部系统：

- 优势 (Strength)： 掌握大量交易和用户数据；直接作用于交易环节，防控能力强。
- 劣势 (Weakness)： 主要面向机构内部，不对公众开放教育；数据和技术应用受限于内部体制和“部门墙”；不专注于面向公众的教育体验。

- 机会 (Opportunity)： 可成为本项目的 B2B 客户，采购定制化教育或分析服务。
- 威胁 (Threat)： 机构自身技术能力的提升可能减少外部合作需求。

传统安全/反欺诈公司：

- 优势 (Strength)： 在特定技术领域（如风险识别、设备指纹、威胁情报）有深厚积累；与机构客户有成熟的合作模式。
- 劣势 (Weakness)： 通常专注于 B2B/B2G 市场，缺乏面向公众的教育和 C 端运营经验。
- 机会 (Opportunity)： 可成为本项目的技术提供商或合作方；可成为本项目的 B2B 客户，采购面向其终端用户的教育服务。
- 威胁 (Threat)： 如果他们也开始进入 C 端教育市场，将是强大的竞争对手。

以下是市场主流反诈应用与本产品的矩阵对比图：

图 6.2-1 市场主流反诈应用与本产品的防御主动性与用户参与度象限图

以下是市场主流反诈应用与本产品的核心功能对照表：

核心功能对比表

核心功能	澄源 (本项目)	国家反诈APP	银行风控系统
AI模拟实战	✓	✗	✗
主动防御训练	✓	✗	✗
游戏化学习	✓	○	✗
知识图谱可视化	✓	✗	○
预警与拦截	○ (训练)	✓ (官方)	✓ (交易)
社区互助	✓	○	✗

图例: ✓ - 核心提供 | ○ - 部分提供/间接相关 | ✗ - 不提供

图 6.2-2 市场主流反诈应用与本产品的核心功能对照

通过对图 6.2-1“防御主动性与用户参与度象限图”和图 6.2-2“核心功能对比表”的深入分析，可以清晰地看出，“澄源（本项目）”在当前市场主流反诈应用中展现出显著且不可替代的创新优势。

首先，在功能层面，“澄源”突破了传统反诈应用的界限，独创性地引入了“AI 模拟实战”和“主动防御训练”两大核心功能。这与“国家反诈 APP”和“银行风控系统”等现有方案形成了鲜明对比，后两者在这些方面均为缺失或未提供。AI 模拟实战使得用户能够在安全可控的环境中，亲身体验和应对各类诈骗场景，极大地提升了实战辨别和应对能力。而主动防御训练则将被动接收警告转变为主动学习和演练，从根本上强化用户的反诈免疫力。

其次，在用户参与度与防御主动性维度，“澄源”的创新优势更为突出。如图 2 所示，“国家反诈 APP”虽然在预警方面有所参与，但其本质仍偏向于被动预警和工具化呈现，用户参与度相对较低。而“银行风控系统”则完全是被动防御，用户基本无感知。“澄源”则凭借其独有的互动性社区和游戏化形式（如核心功能对比表中的“游戏化学习”和“社区互动”），将“防御主动性”和“用户参与度”推向了象限的右上方，实现了“主动训练”的核心目标。通过融入成就系统和任务机制，用户不仅能获得知识，更能在这个过程中享受到学习的乐趣和成就感，从而极大地提升了用户粘性和持续参与的动力。

综上所述，“澄源”不仅仅是在功能上有所增补，更是从根本上重塑了反诈教育和防御的范式。它通过创新的 AI 驱动功能和高度游戏化的互动体验，有效提升了用户的防御主动

性和参与度，使其在同类产品中具备了核心竞争力，奠定了其在未来反诈领域中不可替代的领先地位。

6.3 本项目竞争优势与差异化

创新教育模式： 区别于传统的宣传和案例讲解，本项目采用 AI 模拟、主动防御、游戏化等方式，提供沉浸式、互动性强、趣味性高的学习体验。 旨在解决用户主动学习动力不足、传统教育形式枯燥的问题。

结构化知识体系：基于知识图谱构建和可视化反诈知识，帮助用户系统性、易理解地掌握知识结构，而非碎片化信息。

强调实战与心理： 通过 AI 模拟和主动防御机制，直接训练用户在高压或诱惑情境下的识别和应对能力，针对诈骗者利用心理弱点的核心手段进行训练。

社区互助与激励： 构建用户分享经验、互相学习的社区，结合游戏化激励，形成持续学习和参与的良性循环。

团队独特性： 团队融合了互联网大厂的技术能力和效率与金融行业的业务理解和数据经验，能更深刻地理解诈骗的本质和技术对抗的关键。

七、市场营销与推广策略

7.1 品牌定位与传播信息

品牌定位： 领先的、用户友好的、实战导向的智能反诈教育平台。

传播信息：

- 核心信息：“轻松学反诈，安全不被骗。”或“你的钱袋子，我们帮你守！”
- 价值点信息：“不再害怕诈骗电话，AI 陪你练胆。”“玩游戏，成反诈达人！”“最新骗局，图谱一看就懂。”“加入社区，分享经验，抱团防骗。”“主动提高警惕，让骗子无处遁形。”
- 信任信息： 官方合作（若能达成），技术专业，保护用户隐私。

7.2 营销目标与关键绩效指标

短期目标（例如，上线后 6-12 个月）：

- 获取一定数量的初始用户（例如，达到 X 万注册用户）。 KPI： 用户注册量，用户获取成本 (CAC)。
- 提升用户活跃度。 KPI： 日/月活跃用户 (DAU/MAU)，核心功能（模拟、游戏、社区）使用率。
- 收集用户反馈，快速迭代产品。 KPI： 用户反馈数量，版本更新频率。

中期目标（例如，上线后 1-3 年）：

- 成为特定目标用户群体（如大学生）首选的反诈学习平台。 KPI： 用户满意度，品牌认知度，用户推荐率。
- 探索并初步实现 B2B/B2G 商业化落地。 KPI： B2B/B2G 合作机构数量，合同金额。

- 建立活跃、健康的社区生态。 KPI： 社区发帖量，用户互动率，优质内容产出量。

长期目标： 成为反诈领域的知名品牌，为构建更安全的网络环境做出贡献。

7.3 推广渠道与策略

线上渠道：

- 应用商店优化 (ASO)： 提高在应用商店中的可见度，吸引用户下载。
- 社交媒体营销： 在年轻人聚集的平台（如抖音、B 站、小红书）发布短视频、图文内容，揭露最新骗局，展示产品有趣功能。
- 内容营销： 运营官方博客或合作媒体，发布深度反诈知识、案例分析文章。
- 搜索引擎优化 (SEO)： 优化网站或内容，使用户在搜索反诈信息时能找到平台。
- 付费推广： 针对特定用户群体投放精准广告（需谨慎使用，确保广告内容真实，不引起反感）。

线下渠道：

- 校园合作： 与高校合作开展反诈讲座、活动，将平台作为辅助教育工具。
- 社区推广： 与社区居委会、派出所合作，面向老年人、社区居民进行宣传和推广。
- 合作渠道：
- 与政府/公安部门合作： 争取官方推荐或合作，利用其公信力和渠道推广。
- 与金融/电信机构合作： 提供定制化服务，或通过其渠道向用户推广。
- 与媒体合作： 利用新闻报道、专题节目等提高品牌知名度。

7.4 用户获取、激活、留存策略

获取 (Acquisition)： 突出创新教育模式和有趣体验，吸引厌倦传统模式的用户。 利用合作渠道获取特定群体用户。 优化应用商店展示。

激活 (Activation)： 简化注册登录流程。 设计吸引人的新手引导，快速体验核心功能（如一次 AI 模拟对话，完成第一个游戏关卡）。 首次使用奖励。

留存 (Retention)：

- 持续更新反诈知识图谱和模拟场景，保持内容新鲜感。
- 定期推出新的游戏化挑战和成就，保持学习动力。
- 活跃社区氛围，鼓励用户互动和分享。
- 个性化推荐反诈内容或模拟场景。
- 提供“主动防御式反诈”等独特功能，增强用户粘性。
- 通过 APP 推送最新诈骗预警和平台活动信息。
- 用户激励： 游戏化积分、徽章、成就系统。 社区优质贡献者奖励。 邀请好友奖励。

7.5 销售策略

B2C：

- 基础功能免费，提供增值服务（如更高级的模拟场景、无广告体验、深度报告分析等）收费。
- 谨慎考虑广告模式，若采用需确保不影响用户体验和平台公信力。

B2B/B2G：

- 向政府、金融机构、电信运营商、大型企业提供定制化反诈教育平台或模块。
- 提供反诈数据分析和威胁情报服务（基于知识图谱和用户行为分析，但需注意隐私保护）。
- 为特定行业或群体(如银行员工、老年客户)开发定制培训内容和模拟场景。
- 提供 API 或 SDK，将反诈识别和预警能力集成到其他应用或系统中。

八、盈利模式

“澄源”项目在设计之初便秉持着“守护用户钱袋子”的初心，承诺将核心反诈功能对所有个人用户免费开放。这意味着项目的盈利模式需要围绕非核心个人服务及面向机构的商业合作来构建，以确保项目的可持续运营、技术投入（尤其是大模型 API 调用成本）及持续发展，同时不向最需要反诈帮助的普通用户收取费用。

项目的盈利模式预计将结合面向机构的定制化服务和经过严格筛选的面向个人的补充性收入来源（如谨慎的广告投放）。

1. 机构定制化服务 (B2B 核心)

- 价值主张：利用项目在反诈知识图谱构建、AI 智能体（如 AI 模拟诈骗）及游戏化学习方面的技术积累和创新优势，为对反诈有系统性、专业性需求的各类机构提供定制化解决方案。电信网络诈骗日益猖獗且手段不断翻新，对个人财产安全和社会稳定构成严峻威胁。政府、金融、电信、互联网等行业主管部门依法承担反电信网络诈骗工作的监管主体责任，并需要强化技术反制、预警劝阻和宣传教育。企业和机构也承担风险防控责任，需加强新业务涉诈风险安全评估。因此，市场对专业、高效、智能化的反诈解决方案存在巨大需求。

- 服务内容拓展：

  - 定制版反诈平台或特定功能模块： 基于“澄源”项目的核心技术架构，即强大的反诈知识图谱和 AI 能力，为机构开发或提供可集成到其现有系统中的定制模块。例如：

    - 威胁情报与趋势分析模块： 利用项目持续更新的反诈知识图谱和自动化抽取技术，为机构提供实时的、结构化的诈骗手段、团伙特征、资金流向等威胁情报，并进行深入的趋势分析和风险评估报告。这有助于机构前瞻性地了解诈骗风险，提升精准防

控能力。工商银行就构建了利用知识图谱深度挖掘团伙犯罪关联性的反欺诈系统。

- 风险预警系统： 基于项目积累的对潜在受害者特征的分析 及对诈骗模式的理解，结合机构自身数据（需满足数据安全和隐私要求），开发内部风险预警工具，帮助机构识别潜在的高风险用户或交易行为。这支持了反电信网络诈骗法中强化的预警劝阻要求。

◆ 反诈培训和教育解决方案： 针对机构员工（尤其是金融、电信等行业高风险岗位人员）设计定制化的反诈培训课程和演练方案。

- AI 模拟实战演练： 将“澄源”特色的 AI 模拟诈骗功能 应用于企业内训，让员工在安全可控的环境下体验各种诈骗场景（如冒充领导，冒充客服，虚假投资 等），提高实战识别能力。

- 游戏化学习平台： 利用项目的游戏化学习机制，将机构所需的内部反诈知识（如合规要求、内部流程）融入答题闯关和成就系统，提高员工学习的积极性和知识掌握度。

- 员工反诈能力评估工具： 开发基于学习和模拟结果的评估工具，帮助机构量化员工的反诈能力水平，为培训效果评估和人员管理提供数据支持。

◆ 咨询服务： 基于平台数据（脱敏和聚合后）和技术能力，为行业监管部门、企业提供反诈策略咨询，例如分析特定行业面临的主要诈骗威胁、评估现有防控措施的有效性、提供优化建议等。

■ 目标客户： 政府机构（如公安部门的反诈中心）、金融机构（银行，支付机构）、电信运营商、互联网服务提供商 以及其他可能面临内部欺诈风险或需要对员工进行反诈教育的大中型企业。

2. 精选广告投放 (B2C 补充)

- 原则： 强调广告的“精选”性质，即严格控制广告的数量、内容和投放位置，确保其与反诈主题协调，不干扰用户体验，更要杜绝任何可能被误认为诈骗的信息，维护用户信任。这是一个补充性的收入来源，不应成为主要盈利支柱。

- 广告内容与合作方： 优先选择能够增强用户网络安全、金融安全或提供合法服务的广告：

  - 官方反诈宣传信息或工具推广（如推广国家反诈中心 APP、96110 热线）。

  - 来自有资质的金融机构（银行、证券公司等）提供的正规金融产品或服务信息。

  - 网络安全公司提供的可信安全产品或服务。

  - 其他与提升数字生活安全相关的合法商业广告。

- 投放方式： 非侵入式，例如在学习模块的非核心区域、社区信息流中以“推广”或“合作”形式明确标识展示，或在用户完成特定学习/模拟任务后作为可选信息推送。

3. 数据分析/研究支持 (非直接盈利)

- 原则： 严格遵守《中华人民共和国个人信息保护法》等法律法规，对数据进行严格的脱敏、聚合处理，不涉及任何个人隐私信息。此部分的核心价值在于支持反诈研究、政策制定和行业发展，而非通过数据盈利。

- 输出形式： 提供匿名的、聚合的用户行为数据分析报告（如用户在模拟中最容易受骗的环节、特定诈骗类型的识别难点、学习效果与用户特征的关系等）和平台积累的反诈知识图谱分析洞见。

- 合作对象： 高校研究机构、公安部门、金融监管部门、行业协会等，共同推动反诈理论研究和实践优化。例如，项目的 AI 模拟诈骗和游戏化学习产生的数据，可以为研究不同防范教育方法的效果提供实证支持。

总结：

项目的盈利模式设计旨在平衡社会价值（为个人提供免费反诈服务）和商业可持续性。面向机构提供的定制化解决方案是核心和主要收入来源，这部分利用了项目独特的技术优势和在反诈领域的专业积累，满足了机构在威胁情报、风险防控、员工培训等方面的实际需求。谨慎的广告投放作为补充，数据分析则更多是服务于公共利益和行业发展。这种模式有助于项目在贡献社会的同时，获得持续发展的动力。

九、财务预测

9.1 历史财务数据

鉴于本项目目前尚处于早期开发及准备阶段，历史财务数据相对有限。截至目前，项目尚未产生任何收入。主要的财务支出为支持技术开发和平台运行所需的基础设施成本。

历史收入： 0 RMB

历史支出：

支出类别	具体项目/描述	数量	单位	单价 (RMB)	总价 (RMB)	备注
基础设施	服务器租赁费用	1	月	1,519	1,519	用于早期原型开发、技术测试及数据存储
硬件购置	联想小新 Pro 16 笔记本	8	台	3,200	25,600	为团队成员提供必要的工作设备
人员薪资	项目总监	1	月	5,500	5,500	
	技术负责人	1	月	5,000	5,000	
	数据架构师	1	月	4,500	4,500	
	数据工程师	1	月	4,000	4,000	
	用户体验设计师	1	月	4,000	4,000	
	运营总监	1	月	4,200	4,200	
	市场总监	1	月	4,200	4,200	
	内容策划	1	月	3,800	3,800	
办公及行政	办公用品采购	1	批	800	800	初期基础办公用品
	差旅费	1	批	1,200	1,200	初期市场调研或团队活动
总计					64,319	

净利润： -64,319 RMB

这些历史数据反映了项目在启动阶段对核心技术能力、基础设施、团队建设以及基本运营的初步投入。随着项目进入下一阶段，预计将有更多围绕团队建设、产品开发和市场验证的投入。

9.2 未来 3-5 年收入预测

基于我们对当前反电信网络诈骗严峻形势、全民反诈宣传教育的政策导向以及市场对创新型反诈工具需求的分析，本项目未来的收入增长潜力主要来源于以下几个关键领域，并预计在未来 3-5 年内逐步实现和加速增长：

B2C 用户价值实现 (广告等)： 随着用户规模的增长和活跃度的提升，应用将具备基于用户流量的广告变现潜力。中国的互联网用户基数庞大，且网购等行为已深入人心，但网络安全问题依然突出，用户对提升自身安全意识有内在需求。通过提供寓教于乐的内容和互动方式，我们有信心吸引并留住大量个人用户，从而为广告业务奠定基础。预计这部分收入将在项目获得初步用户规模后（例如，在推广和社区运营取得成效的第二年或第三年）开始贡献，并随用户增长呈加速趋势。

B2B/G 定制化服务与技术输出： 这是我们预计在早期即可开始探索并有望贡献稳定收入的核心途径。

金融机构与电信运营商： 《中华人民共和国反电信网络诈骗法》明确要求金融机构和电信业务经营者承担反诈风险防控和宣传教育责任。我们的平台能够提供用户友好的反诈教育内容、互动模式和数据分析洞察，可以作为这些机构满足合规要求、提升客户防诈能力的有效工具。特别是平台基于知识图谱和 AI 的技术能力，与金融机构在反欺诈风控领域的先进技术应用趋势高度契合。我们可以提供定制化的技术接口、数据服务（在严格遵守合规和隐私要求下进行脱敏、聚合）或集成化教育模块。预计这部分收入可以在项目产品成熟度达到一定水平后（例如，在第一年下半年或第二年）通过试点合作逐步实现。

政府相关部门： 反诈工作是国家战略，官方平台已投入使用。然而，社会层面依然需要更广泛、更有效、更受欢迎的宣传教育补充官方体系，构建全社会反诈氛围。我们的平台因其互动性和趣味性，有望成为国家“全民反诈在行动”和“五进”活动的有力支持。可以通过合作、采购服务甚至未来纳入公共服务体系的方式实现价值。预计合作模式和收入贡献将在项目获得社会认可度和影响力后逐步显现（例如，在第二年或第三年）。

在线教育平台： 平台的核心是将反诈知识有效地进行传播和学习，其游戏化和可视化能力可以作为新增内容模块或产品线，与现有在线教育平台合作。人工智能在安全教育中的应用也被认为是提升效率和互动性的方向。这部分收入潜力将在验证平台教育效果后进一步释放。

未来收入预测 (示例性，基于假设)：

预测年份	预测阶段	收入增长驱动因素	预测年收入 (万元 RMB)	累计收入 (万元 RMB)
年 1	启动及早期验证	少量 B2B/G 试点项目	5-15	5-15
年 2	用户增长与 B2B 拓展	B2C 用户流量初步增长，扩大 B2B/G 客户群体，探索合作模式	50-150	55-165
年 3	规模化与模式成熟	B2C 广告收入显著增长，B2B/G 服务标准化及规模化推广，形成稳定合作	200-500	255-665
年 4	加速增长	用户爆发式增长，B2C 收入规模效应显现，B2B/G 客户群扩大及客单价提升，探索新服务	600-1200	855-1865
年 5	持续扩张与深化	巩固市场地位，收入来源多元化，技术能力持续领先，拓展至相关安全教育领域	1500-3000+	2355-4865+

9.3 未来 3-5 年成本预测

随着项目从开发阶段迈向运营和增长阶段，成本结构将发生显著变化并大幅增加。主要的成本构成和预测增长趋势如下：

技术基础设施成本： 包括服务器租赁、带宽、存储等费用。这部分成本将与用户规模、数据量（如知识图谱的扩展、用户行为数据）直接相关，随着业务发展呈线性或非线性增长。例如，AI 模型训练和推理所需的计算资源是重要的技术成本。

人员成本： 项目团队的核心资产是人才，特别是具备全栈开发、数据分析以及 AI/知识图谱等专业技能的团队成员。随着项目规模扩大、功能增加、用户服务需

求增长以及商业拓展的需要，需要持续招聘技术、运营、市场、销售及管理人员。这部分将成为未来几年最大的成本支出。

市场营销和用户获取成本： 为了快速扩大用户规模和提升品牌影响力，需要进行线上线下推广活动。获取 B2B/G 客户也需要销售和市场推广投入。这部分成本在项目初期和快速增长期会相对较高。

研发投入： 持续投入对知识图谱、AI 算法等核心技术的迭代优化，开发新功能（如模拟实战、社区互动），以及反诈知识内容的更新和丰富，以保持技术领先和内容吸引力。

运营和客户服务成本： 社区管理、用户支持、内容审核、日常行政管理等。

合规和法律成本： 随着用户数据量增加和业务模式复杂化，确保严格遵守《个人信息保护法》、《反电信网络诈骗法》等法律法规至关重要，这需要投入相应的法律和技术资源。

其他成本： 办公场所租赁、差旅、税费等。

未来成本预测 (示例性，基于假设)：

预测年份	预测阶段	成本增长驱动因素	预测年成本 (万元 RMB)	累计成本 (万元 RMB)
年 1	启动及早期验证	基础设施、核心团队薪酬、少量市场投入	50 -100	50-100
年 2	用户增长与 B2B 拓展	技术设施扩展、团队规模扩大、市场推广力度加大	200-400	250-500
年 3	规模化与模式成熟	技术设施与人员成本进一步增加，规模化运营，市场营销费用维持高位或略降	500-1000	750-1500

年 4	加速增长	应对用户爆发式增长的技术和运营压力，团队持续扩张，加大研发投入	1000-2000	1750-3500
年 5	持续扩张与深化	基础设施和人员成本随规模增长，但增长率可能放缓，研发和新业务拓展投入	1800-3500+	3550- 7000+

9.4 利润预测与现金流预测

利润预测：

初期亏损： 在项目启动和早期增长阶段（例如，年 1-年 3），由于收入尚未形成规模，而技术研发、团队建设和市场推广需要较大投入，预计项目将出现持续亏损 37。这是大多数科技型初创企业为追求未来高增长而经历的常见阶段。

盈亏平衡与盈利： 随着用户规模和商业模式的成熟，特别是 B2B/G 服务的稳定收入和 B2C 广告收入的增长，收入增长速度预计将超过成本增长速度。我们预测在项目运营的第 3 年或第 4 年，有望实现盈亏平衡，并在随后的年份实现盈利。利润水平将取决于收入规模、成本控制能力和商业模式的效率。

现金流预测：

负现金流与资金需求： 在亏损期间，项目将面临负现金流，即支出大于收入 3637。这将是项目对外部融资产生需求的核心原因。持续的现金“消耗”需要通过融资来补充，以支持项目的持续运营和发展。

现金流转正： 当项目实现稳定盈利并能产生正向经营性现金流时，将不再依赖外部融资来维持日常运营，进入健康发展的轨道。这通常发生在实现盈亏平衡之后。

利润与现金流预测 (示例性，基于假设)

预测年份 (年)	预测年收入 (万元 RMB)	预测年成本 (万元 RMB)	预测年利润 (万元 RMB)	累计利润 (万元 RMB)	预测年现金流 (示例)	累计现金流 (示例)
年 1	5-15	50-100	-45 至-85	-45 至-85	负，需融资	负，需融资
年 2	50-150	200-400	-150 至-350	-195 至-435	负，需融资	负，需融资
年 3	200-500	500-1000	-300 至 0	-495 至-435	负/接近平衡，需融资	负，需融资
年 4	600-1200	1000-2000	-400 至+200	-895 至-235	负/正，需融资/可自持	负/接近平衡，需融资
年 5	1500-3000+	1800-3500+	-300 至 +1200+	-1195 至+965+	正，可自持/产生盈余	负/正，取决于融资量

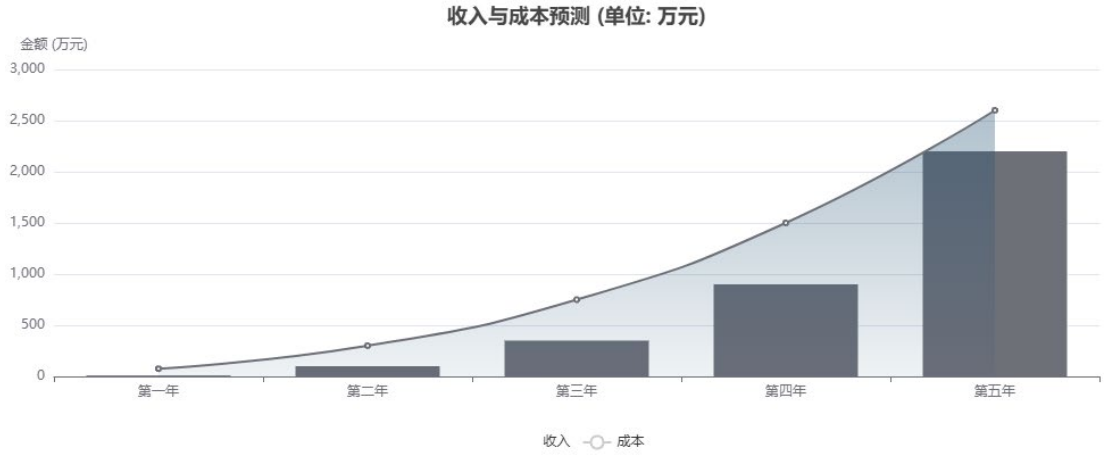

图 9.4-1 收入与成本预测

9.5 估值与融资需求

基于上述财务预测和项目的市场潜力，我们明确了项目的估值基础和融资需求：

融资需求： 为了弥补早期运营的负现金流、加速产品开发、扩大市场份额、建立团队以及抓住市场机遇，本项目需要外部资金支持。总融资需求将根据详细的现金流预测和未来发展计划进行精确测算，预计需要覆盖从启动到实现正向现金流期间的累计资金缺口，并预留一定的缓冲资金。这笔资金将主要用于：

（1）核心技术团队的扩充和薪酬支付

（2）知识图谱和 AI 模型的进一步研发和优化

（3）平台功能开发、内容生产和用户体验优化

（4）市场推广和用户获取活动

（5）B2B/G 市场拓展和销售团队建设

（6）日常运营和行政开支。

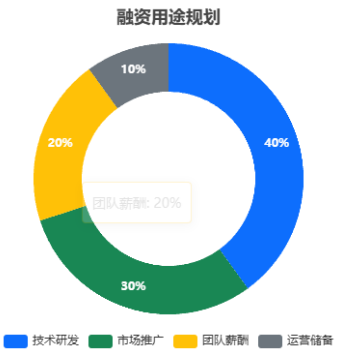

图 9.5-1 融资用途规划

估值： 项目目前处于早期阶段，尚无成熟产品和规模化收入，传统基于利润或收入的估值方法适用性有限。本项目的早期估值将主要基于其**未来发展潜力、技术创新性、所处市场的巨大社会价值和商业机会、核心团队的经验与能力**，以及已获得的初步市场验证（如用户反馈、潜在合作意向）。我们认为，项目的知识图谱和 AI 技术壁垒、独特的游戏化教育模式、以及在反诈这一国家战略领域的先发优势和 B2B/G 市场潜力，构成了其核心价值基础。估值应反映其作为潜在战略收购目标所具备的长期价值。早期融资轮次通常是种子轮或天使轮，估值更多是基于市场对类似项目潜力的判断以及谈判结果。

融资目的： 本轮融资旨在为项目提供启动资金或加速发展所需的燃料，帮助项目迅速搭建核心产品、获取早期用户、验证商业模式，并为后续更大规模的融资或退出打下坚实基础。风险投资作为一种专门投资于新创意和新技术企业的高风险、高收益并存的投资形式，与本项目的性质高度契合，将是我们优先考虑的融资来源。

十、风险分析与应对策略

10.1 技术风险与应对

风险：诈骗技术快速迭代，现有反诈技术可能失效。知识图谱构建和维护、AI 模型的准确性和鲁棒性面临挑战。

应对：建立持续的威胁情报收集和分析机制。投入研发，跟踪前沿技术（如 LLM 在反诈中的应用）。 采用敏捷开发方法，快速迭代产品功能。 加强与安全技术社区的交流与合作。

10.2 市场风险与应对

风险： 用户获取困难，尤其是在教育产品领域。 竞争激烈，特别是来自官方平台。 用户对平台效果的怀疑或教育意愿不足。

应对： 突出产品在用户体验和教育效果上的独特价值。 制定精准的市场营销和推广策略，触达目标用户。 加强与政府、学校、社区等合作，利用其渠道和公信力。 持续收集用户反馈，优化产品，提升用户粘性。

10.3 运营风险与应对

风险： 社区内容质量控制和管理（如出现虚假信息、广告甚至新的诈骗苗头）。 如何持续生成吸引用户的新鲜内容（诈骗案例、科普）。

应对： 建立严格的内容审核机制和社区管理规范。 智能机器人辅助内容聚合和过滤。 激励用户分享真实经验，结合专家引导。 建立高效的内容更新和维护流程。

10.4 数据安全与隐私风险与应对

风险： 处理用户个人信息和学习行为数据可能面临隐私泄露风险。 合规风险，需要遵守相关法律法规（如《网络安全法》、《个人信息保护法》、《反电信网络诈骗法》）。

应对： 建立高标准的数据安全保障体系，包括数据加密、访问控制、安全审计等。 严格遵守相关法律法规，获取用户明确授权，并在隐私政策中清晰说明数据收集和使用方式。 对敏感数据进行匿名化或假名化处理。 “主动防御式反诈”功能需明确承诺不获取或损害用户数据。 定期进行安全审计和合规审查。

10.5 财务风险与应对

风险： 融资不确定性。 商业模式落地和盈利不及预期。 成本控制不当。

应对： 制定合理的融资计划和资金使用规划。 验证并优化商业模式，探索多样化收入来源。 精细化运营，控制各项成本。 准备好备用方案以应对资金压力。

10.6 退出策略

对于我们开发的这款反诈平台应用，结合其技术创新性（知识图谱、AI）、独特的互动模式（游戏化、社区）以及显著的社会价值（提升全民反诈意识），其未来的发展路径和投资者价值实现方式至关重要。我们认为，最具有战略意义和现实可行性的退出策略是战略性收购（Strategic Acquisition）。此外，我们也考虑首次公开募股（IPO）和管理层收购（MBO）作为可能的长期选项，但鉴于项目当前阶段和行业特点，战略性收购是首要聚焦的退出方向。

战略性收购

我们认为，本应用的核心技术能力、用户基础、数据洞察潜力以及在反诈宣传教育领域的独特方法，对多个行业的大型机构具有强大的吸引力，是实现投资回报和项目价值最大化的主要途径。

- 潜在的战略收购方及驱动因素

大型科技/互联网公司： 许多大型科技公司拥有庞大的用户群体，也面临平台上的欺诈风险，急需提升自身安全防护能力和用户反诈意识。我们的核心技术，如基于知识图谱的复杂关系识别和 AI 驱动的风险分析能力，与这些公司在安全风控、设备反欺诈 等领域的布局高度契合。通过收购，他们可以整合先进的反

诈技术，获取用户教育能力，并在合规框架下利用脱敏数据优化其风控体系，同时获得一支具备全栈开发和数据分析经验的技术团队。例如，工商银行已在其设备反欺诈系统中创新应用知识图谱和人工智能等前沿技术，成功识别和打击团伙欺诈。

金融机构/电信运营商： 《中华人民共和国反电信网络诈骗法》明确要求金融机构、电信业务经营者、互联网服务提供者承担风险防控责任，并加强对用户的反诈宣传教育。我们的应用能够提供用户友好、生动有趣的反诈教育内容和互动模式，这正是这些机构在满足合规要求、提升客户防诈能力方面的迫切需求。调查报告也显示，公众对网络购物安全和维权存在痛点，对提升自身安全意识有需求。如果应用能有效提升用户识别和防范诈骗的能力，将被视为重要的 B2B 服务或内部/外部宣传教育工具。

在线教育平台/内容提供商： 本质上，我们的应用是一个高效的知识传播和学习平台。其游戏化学习模式 和知识可视化能力 可以极大地丰富现有在线教育平台的内容形式和用户体验。反诈知识是一个具有广泛需求和社会价值的垂类内容，可以作为新增业务线或产品模块进行整合。人工智能在安全教育培训中的应用也显示出提升效率和互动性的潜力。

政府相关部门或其合作机构： 反诈工作已上升为国家战略。尽管国家反诈中心等官方平台已投入使用，但一些官方工具在用户体验或推广方式上存在争议。一个自愿使用、寓教于乐且被证明有效的第三方平台，能够有力补充官方“全民反诈”宣传教育体系（如“五进”活动），构建全社会反诈氛围。虽然不一定是纯商业收购，但也可能通过政府注资、指定合作、并购入官方体系等多种形式实现价值整合，从而实现公共利益和项目价值的双重回报。

- 提升战略收购价值的关键要素

强化技术壁垒： 持续迭代和优化基于知识图谱和 AI 的核心技术，特别是 AI 对热点诈骗信息的实时抽取、分析和反制能力，构建难以复制的技术优势。例如，利用 AI 模拟诈骗实战和“主动防御式反诈”功能 等创新模式。

扩大用户规模及提升活跃度： 通过持续提供优质内容、优化游戏化体验和社区运营，吸引并留住大量用户。高用户量和活跃度是产品市场吸引力和用户粘性的直观体现，也是收购方高度看重的指标。

验证和拓展商业模式： 积极探索和发展 B2B 服务，向金融机构、电信运营商、教育平台等提供定制化反诈协助或技术服务。稳定的商业收入将有力证明项目的盈利潜力和市场可行性。

积累合规有价值的数据资产： 在严格遵守《个人信息保护法》、《反电信网络诈骗法》等法律法规，确保用户隐私安全的前提下，通过对用户行为、学习路径、风险偏好等数据进行脱敏、聚合分析，提炼出有价值的行业洞察和反诈策略，这部分“数据智能”对于收购方提升自身业务能力具有重要价值。

塑造正面品牌形象： 建立一个可靠、权威、用户信赖且有社会影响力的反诈品牌。在反诈领域，信任是用户采纳和持续使用的基石。

确保全面合规性： 严格遵守所有相关的法律法规，包括个人信息保护、内容发布、应用备案等要求。合规是项目持续运营和被收购的基础。

附录 (Appendix)

[1] 智能反诈演练 WEB 平台 V1.0.0　　软著　　正在申请

[2] 智能反诈演练 APP V1.0.0　　软著　　正在申请