4.项目环境

4.1操作环境

4.2涉众分析

5.数据获取

5.1 问卷形式的数据采集

5.2 其他途径的硬数据采集

5.3 数据分析

5.4 用户的担忧与建议

5.5 总结

**4 项目环境**

**4.1 操作环境**

1.数据库：采用MySQL、MongoDB等存储用户、交易和行为数据，支持高效查询与风险分析，且需要有一个包含已知诈骗模式和历史案例的数据库，以便系统可以基于这些数据进行学习和识别。

2.机器学习算法：利用XGBoost、LSTM等算法检测诈骗模式，结合无监督学习进行异常行为识别。

3.数据采集程序：通过API、爬虫和日志采集工具（Kafka/Flume）收集诈骗相关数据，并将这些数据用于模型训练和模式识别。

4.模型管理与更新：需要对模型进行管理和更新以保证其精度和效率。

5.前端界面：构建用户友好的交互界面，展示风控预警和反诈信息。

6.后台处理程序：采用Java/Python构建高并发处理系统，实现风控规则计算与数据分析。

7.安全保障：结合SSL加密、防火墙、风控策略等多层防御机制确保系统安全。

8.系统运维程序：利用Prometheus、ELK等工具进行日志监控、故障自动恢复和系统优化。

**4.2 涉众分析**

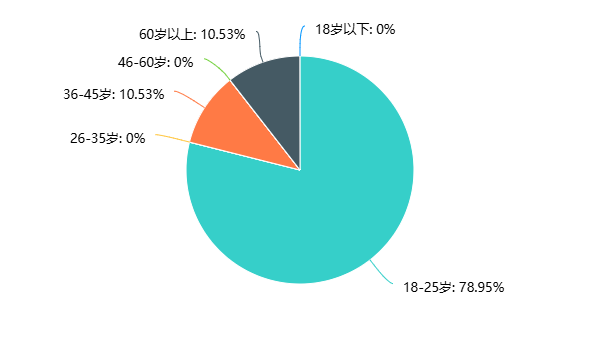
|  |  |  |
| --- | --- | --- |
| 涉众 | | 需求 |
| 用户 | | 1. 通过系统识别诈骗行为 2. 获取案例分析，提高防骗意识 |
| 反诈工作人员 | | 1. 建立诈骗数据库，形成反诈模型 2. 实现公安、银行、社交平台等部门信息联动，快速锁定诈骗团伙 3. 共享诈骗分子信息，对高危账户、手机号、IP地址等进行封禁 |
| 反诈骗系统的技术团队 | 维护人员 | 1. 保障系统稳定运行，避免宕机和服务中断 2. 定期更新系统，修复漏洞，优化性能 |
| 数据管理人员 | 1. 分析诈骗模式，训练AI模型，提高识别准确率 2. 维护黑名单数据库，实现跨机构数据共享 |
| 安全管理人员 | 1. 保护系统免受黑客攻击，防止数据泄露 2. 加强账号安全，防止诈骗分子伪装或劫持账户 |
| 经营管理人员 | 1. 负责系统投资、成本控制、收益评估，评估行业合作、推广投入的性价比 2. 促进行业合作，与公安、银行、社交平台联动 |
| 政府监管机构 | | 1. 建立全国性诈骗分子、账户、电话等信息库 2. 需要对系统的法律合规性进行监管，保障系统合法合规运作 |

**5 数据获取**

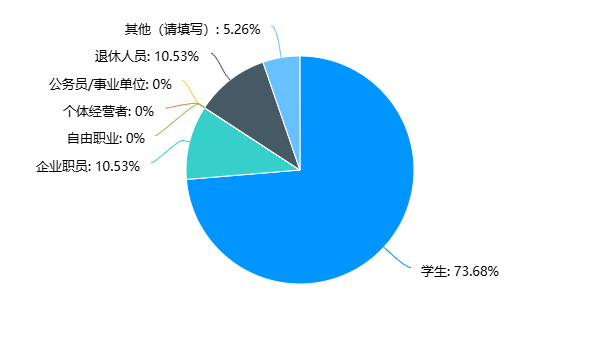
**5.1 问卷形式的数据采集**

问卷形式采集得到的数据主要以图表的形式进行展示。

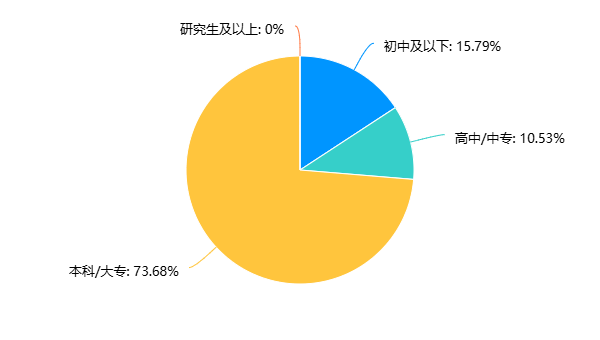
1. 年龄

****

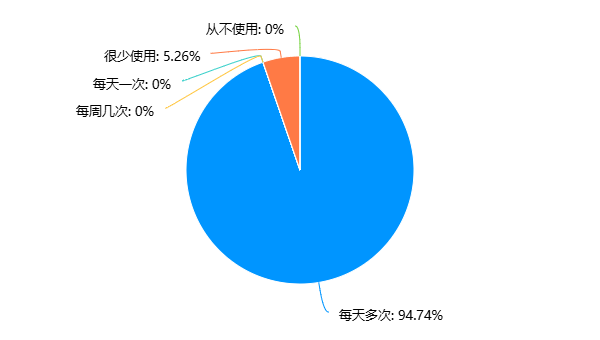
1. 职业



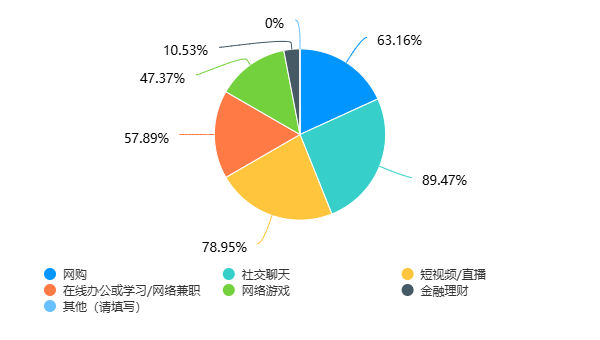
1. 学历



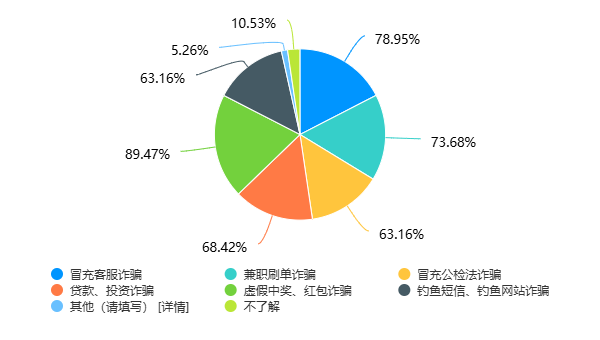
1. 使用互联网和智能手机的频率



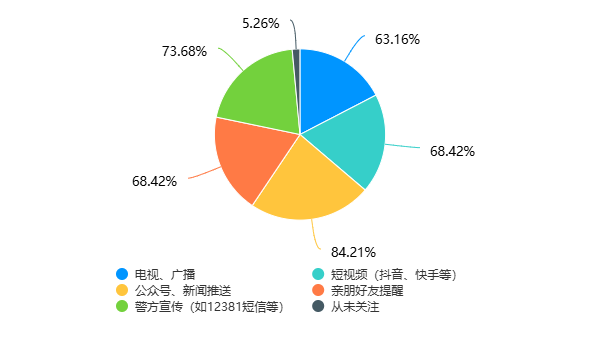
1. 主要在互联网进行的活动



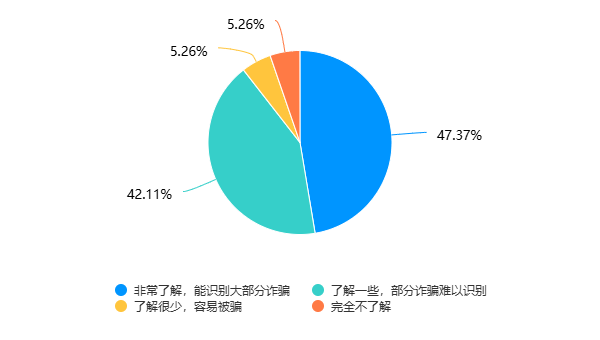
1. 是否了解常见的电信诈骗类型



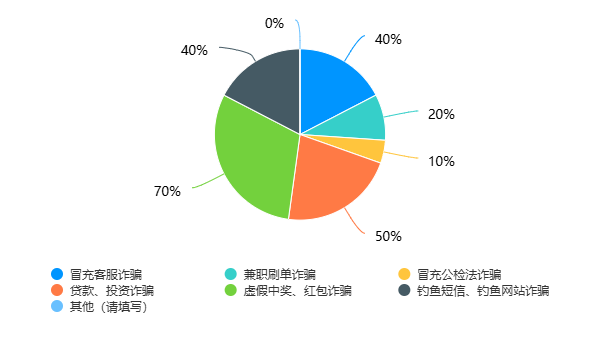
1. 是否关注或接受过反诈宣传



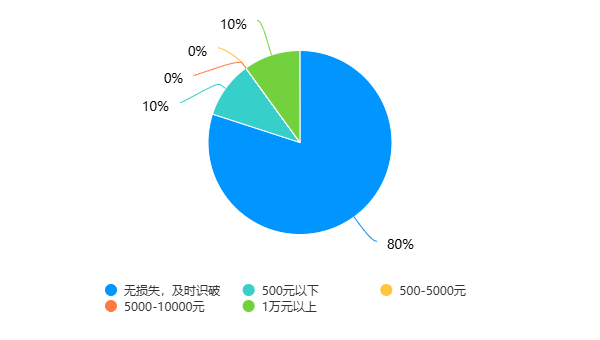
1. 觉得自己的防诈能力如何



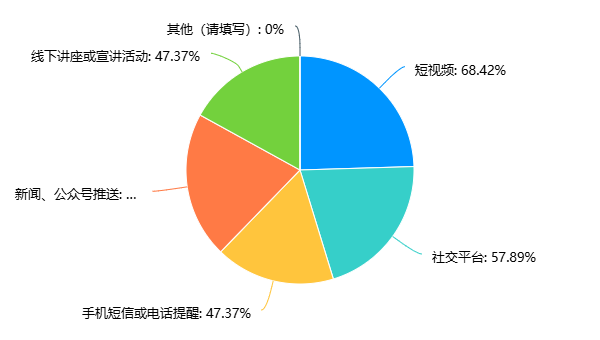
1. 曾遭遇的诈骗类型



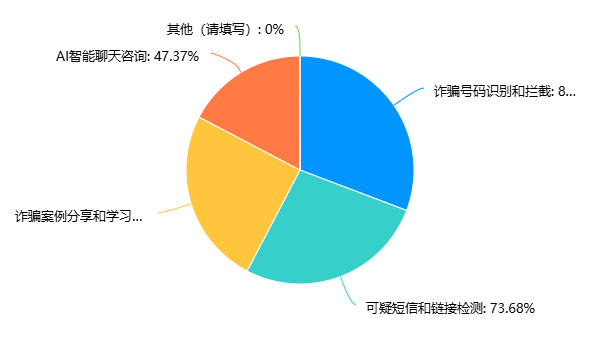
1. 诈骗导致的损失金额



1. 希望通过哪些方式获得防诈骗信息



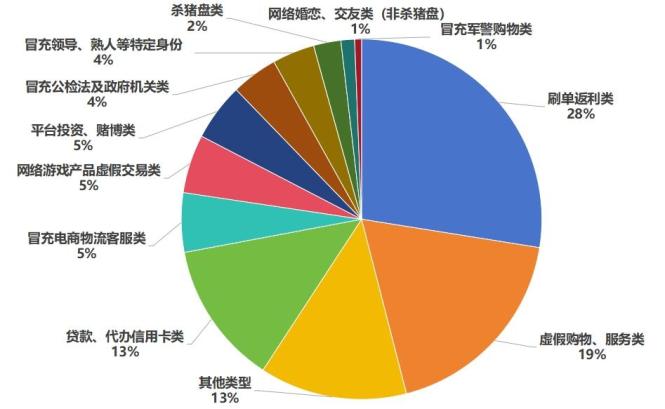
1. 觉得以下哪些功能有帮助

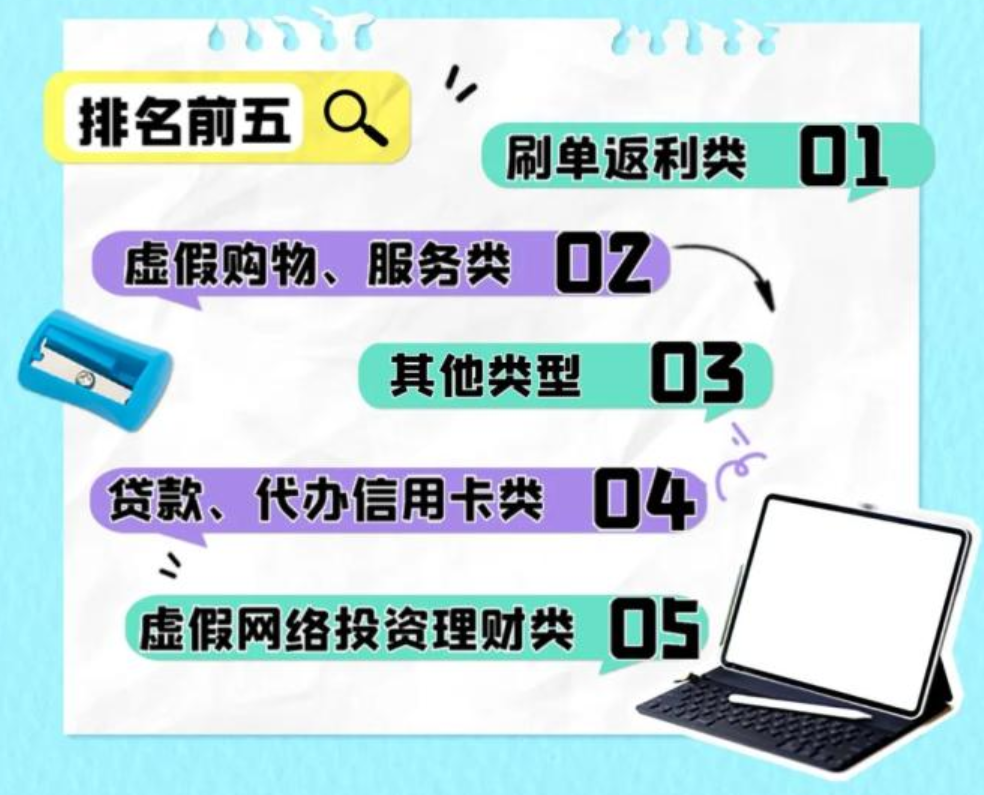


**5.2 其他途径的硬数据采集**

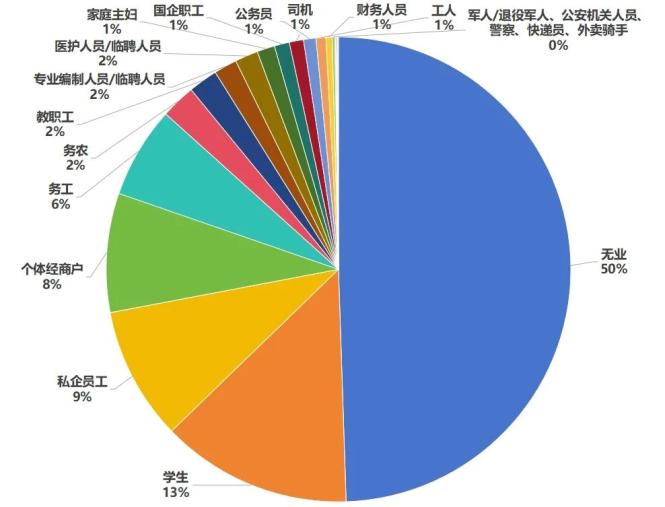
为了弥补问卷采集收集到软数据偏多、硬数据偏少的问题，我们进一步从相关平台和app的年度报告中查找相关数据。

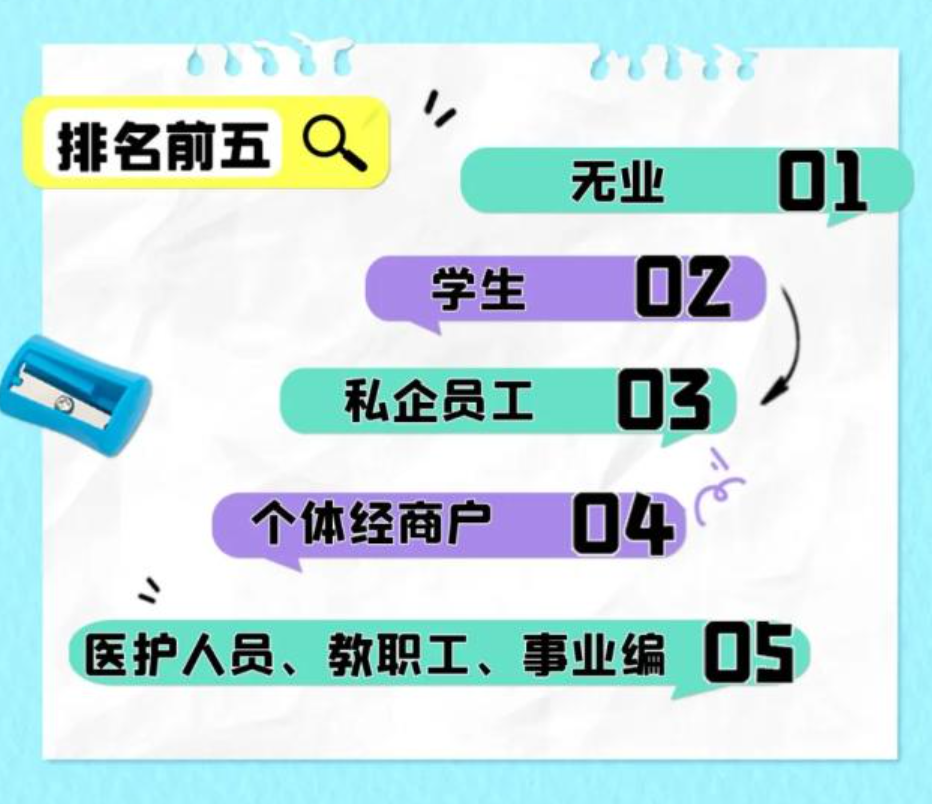
诈骗类型

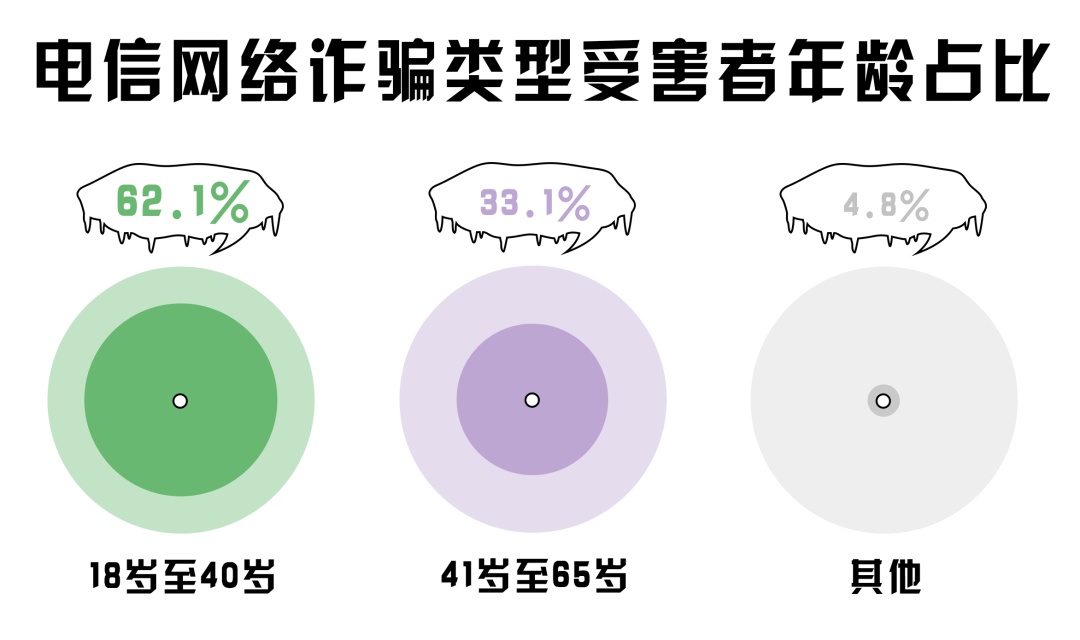




高发被骗群体









数据显示，电信诈骗的主要受害群体为18至40岁的无业人员（占50%）和学生（占13%），刷单返利（28%）和虚假购物（19%）是最常见的诈骗类型。反诈宣传在社交媒体上反响强烈，相关话题阅读量超千万，显示公众防诈意识正在提升，但仍需针对年轻人和高风险职业加强教育，以遏制诈骗高发态势。

**5.3 数据分析**

当前电信诈骗形势严峻，诈骗分子利用受害者的投机心理、贪念和欲望实施犯罪，涉案金额巨大，社会危害触目惊心。数据显示，18至40岁的无业人员（50%）和学生（13%）是最主要的受害群体，而刷单返利（28%）、虚假购物（19%）和虚假投资理财等诈骗形式尤为猖獗。尽管现有的反诈平台（如国家反诈APP、抖音小安等）已具备基础预警功能，但用户调研表明，公众对更智能、更高效的反诈工具需求迫切。

未来，融合AI、大数据、区块链及元宇宙等前沿技术的智能反诈平台将成为发展趋势。这类平台不仅能实时识别和阻断诈骗行为，还能通过深度学习不断优化反诈模型，尤其针对"刷单返利""杀猪盘""虚假贷款"等高发诈骗类型进行专项防控。此外，平台可通过分析诈骗数据动态调整策略，提升预警精准度，同时利用虚拟现实技术模拟诈骗场景，增强公众防骗意识。

这一领域不仅具有显著的社会价值，还蕴藏巨大的市场潜力。随着技术迭代和用户需求升级，智能反诈平台有望成为数字时代的安全基础设施，为公众提供全方位、多层次的防护，有效遏制电信诈骗的蔓延态势。

**5.4 用户的担忧与建议**

用户对现有反诈平台也存在诸多顾虑：一是担心政府过度收集个人信息，侵犯隐私权；二是系统更新滞后，难以应对新型诈骗手段；三是智能化程度不足，无法精准识别诈骗电话和推销电话；四是部分地区存在强制安装现象，引发抵触情绪。多数用户期望平台能在保护隐私的前提下，通过技术创新实现更精准的诈骗识别和拦截。

**5.5 总结**

电信诈骗已成为当前数字化社会面临的重大安全挑战，其危害程度之深、影响范围之广令人警醒。数据显示，18-40岁的年轻群体，特别是无业人员（占比50%）和学生群体（占比13%）最容易成为诈骗目标。从诈骗类型来看，刷单返利（28%）、虚假购物（19%）和虚假投资理财等诈骗手段最为猖獗，诈骗分子往往利用受害者的投机心理和贪念实施犯罪，造成的经济损失和社会影响触目惊心。

当前，以国家反诈APP为代表的防范平台已初步建立起预警防护体系，但用户反馈显示，现有平台仍存在诸多亟待改进的问题。首要问题是用户对个人信息安全的担忧，担心政府过度收集隐私数据；其次是平台更新滞后，难以应对层出不穷的新型诈骗手法；再者是智能化程度不足，无法精准识别诈骗电话和推销信息；此外，部分地区强制安装的做法也引发了一定程度的抵触情绪。这些反馈凸显出公众对更智能、更人性化反诈工具的迫切需求。

面向未来，反诈平台的发展需要把握技术创新与隐私保护的平衡点。通过整合AI、大数据分析和区块链等前沿技术，构建更智能的识别系统；采用联邦学习等隐私计算技术，在保护用户数据安全的前提下提升识别精准度；建立动态更新机制，重点打击高发诈骗类型；同时优化用户体验，避免强制安装等可能引发抵触的做法。只有做到技术先进性与人文关怀并重，才能真正赢得公众信任，使反诈平台发挥应有的防护作用。

从更宏观的视角来看，智能反诈平台的建设不仅具有重要的社会价值，也蕴含着巨大的市场潜力。一个理想的智能反诈系统应当实现多重平衡：在安全防护与隐私保护之间、在强制防护与自愿使用之间、在技术创新与操作简便之间找到最佳结合点。这需要政府部门、科技企业和公众的共同努力，通过持续的技术创新和制度完善，最终构建起数字时代的安全防护网，为人民群众的财产安全保驾护航。