AI 筑牢邮件安全防线 永赢基金以大模型守护金融数字资产

在数字化深度渗透的公募基金行业，电子邮件承载着投研决策、客户服务、监管报送等高价值敏感数据，是业务开展的核心基础设施，却也成为网络攻击的“头号突破口”。随着生成式 AI 技术的普及，钓鱼攻击愈发智能化、隐蔽化，加密附件、二维码伪装、账号仿冒、社会工程学诱导等高级威胁层出不穷，传统防护手段日渐乏力，给基金公司的安全运营带来严峻挑战。

永赢基金积极践行公募基金行业网络和信息安全防护要求，通过安全 GPT 钓鱼检测大模型，以人工智能技术重构邮件安全防御体系，打造“AI 驱动、全链路覆盖、智能化研判”的安全防护屏障，用科技力量守护公司数字资产与投资者合法权益。

这套智能防御体系，如同一位 7×24 小时在线的专业安全专家，突破了传统规则检测的局限，具备三大核心优势：一是深度意图理解能力，能够像人一样“读懂”邮件上下文逻辑，精准识别仿冒监管、财务付款、账户异常等社工话术，区分正常业务邮件与高仿钓鱼邮件；二是多模态检测能力，实现文本、附件、链接、二维码、HTML 页面的一体化检测，能够穿透加密压缩包、白链接跳转、HTML 走私等高级伪装，捕捉隐藏的恶意载荷；三是自动化协同能力，通过 AI 智能体自动调度检测工具，完成复杂攻击的自动化研判、分级处

置与链路还原，大幅降低人工依赖。

上线运行以来，永赢基金邮件安全能力得到显著提升：高对抗钓鱼邮件检出率超 93%，传统网关漏报的高级威胁被批量捕获，误报率降至 0.28%以下；安全人员人工复核工作量减少 80%以上，从繁重的邮件复核中彻底解放，专注于高阶威胁狩猎与安全运营优化。

作为 AI 大模型落地邮件安全的实践，永赢基金以技术创新驱动安全升级，有效防范了各类钓鱼攻击风险。未来，永赢基金将持续深化人工智能、大数据等新技术在网络安全领域的应用，不断完善主动防御、智能研判、快速闭环的安全体系，为投资者提供更可靠的安全保障。