提高全员网络安全意识，筑牢企业网络安全防线：民生加银基金网络安全普及实践

网络安全宣传普及

民生加银基金管理有限公司

2024 年 9 月

目　录

摘　要 3
一、背景意义 3
二、主要做法 4
三、实践成效 15
四、经验启示 17
参考文献 17

摘　要

民生加银基金管理有限公司引入第三方安全意识教育托管服务，针对公司员工进行网络安全宣传普及，以自动化安全教育管理平台为主要工具，使网络安全意识教育与钓鱼邮件实战演练相结合，持续为企业数字资产和业务运营安全提供保障。

通过本次项目构建个性化、智能化的网络安全教育体系，赋能安全团队，快速、高效地开展覆盖全员的网络安全意识教育，实现人为风险因素管理，降低员工数字风险行为，并逐步打造企业网络安全文化。

关键词：网络安全意识教育，自动化安全教育管理平台，网络安全文化

一、背景意义

金融证券行业的网络和信息安全直接关联到国家金融安全和市场稳定。随着数字化转型，随着金融服务的线上化，公司业务越来越依赖于网络系统。而当今网络安全威胁日益严峻，特别是以“人”为突破口的非技术性攻击成为主流方式，可能直接威胁到客户资产安全和公司声誉。

从国家法律法规及监管趋势来看，《网络安全法》《数据安全法》《金融消费者权益保护实施办法》《个人金融信息保护技术规范》《金融数据安全 数据安全评估规范》等均对金融证券领域的网络安全、数据安全、个人信息保护等方面的安全合规与意识教育工作提出了明确要求。

通过定期的安全意识培训，提高员工对网络安全的认识，使员工能够识别并防范潜在的网络威胁，保障公司业务的稳定运行和客户信息的安全。但传统的网络安全教育往往采用线下培训、考试等形式，教育效果难以量化，且很难切实影响员工行为。公司若自行生产教育内容，生产周期长、成本高，容易缺乏时效性。公司开展安全意识全员教育工作，缺乏相应的教育内容及工具平台等资源。

公司引入第三方安全意识教育服务，以自动化安全教育管理平台为主要工具，使意识教育与实战演练相结合，配合线上线下活动运营，构建个性化、智能化的安全教育体系，降低员工数字风险行为，并逐步打造企业数字安全文化。赋能安全团队，快速、高效地开展覆盖全员的网络安全意识教育，实现人为风险因素管理，持续为企业数字资产和业务运营安全提供保障。

二、主要做法

（一）教育痛点

1.教育内容尚未体系化：

安全意识教育未形成系统化，员工缺乏全面的、结构化的安全知识框架，容易形成风险敞口。不同岗位员工培训不均衡、较零散或随需而做，“一刀切式”培训内容缺少个性化与针对性。课程时间较长占用工作时间，培训内容过于理论或枯燥，不易于理解、吸收和消化，使培训成了走马观花、被动应付。

2.效果评价未能可视化：

培训中习得的知识和技能缺乏实用性，缺少动手能力，难以迁移到工作中。培训评估与考核往往停留在考试通过率与培训参与度等学习层评估，缺少全面的、客观的度量评估机制，对行为层、结果层缺乏有效跟踪与评估。即便达到宣传目的，仍不能从“知规”转化为“守规”，难以实现安全培训与企业安全文化的良性循环。

（二）总体设计

网络安全意识教育是一项集网络安全、风险管理、成人教育、心理学与行为学、传播与营销学等跨多学科领域的工程。本次项目基于安全意识教育方法论“计划-评估-实施-度量-优化”，以员工为本，通过安全意识教育“四化”策略，将安全意识工作扎实落地。

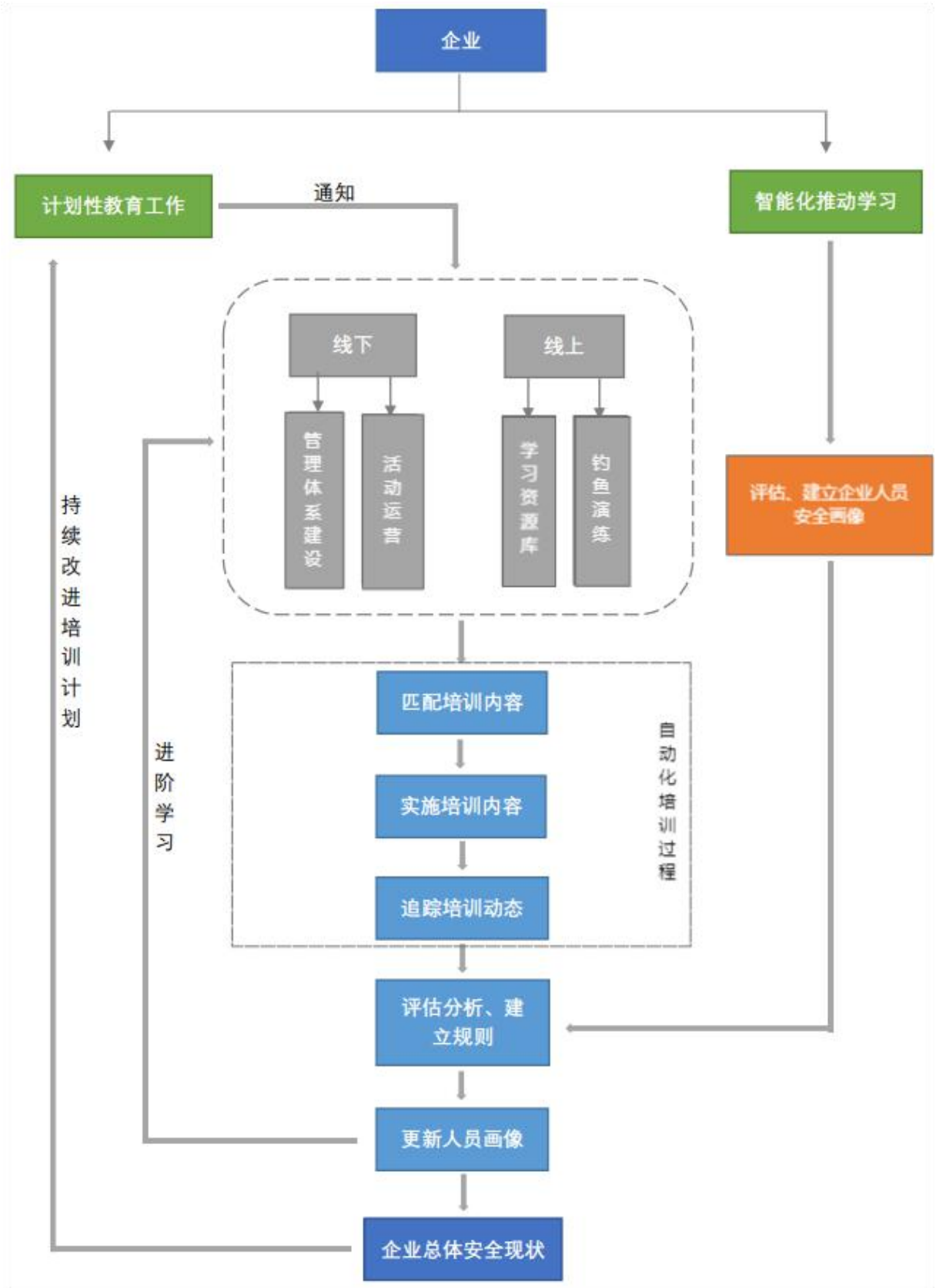

图 2-1 安全意识教育总体设计

1.体系化：教育内容建设

通过系统性、针对性、主题化的网络安全培训内容，持续为全体员工与技术人员赋能，全面提升全体员工的信息安全综合素养，确保员工理解各项安全管理制度与规范，防范因人为因素导致的违规事件与安全风险。同时，提升技术人员的安全专业能力，弥补意识与技能差距，并在全行范围内达成一致共识，为整体安全能力与保障水平提升打开良好的基础。

2.实战化：钓鱼邮件演练

以练促防，通过常态化开展贴近真实攻击的钓鱼模拟演练，进一步提升和检验员工精准识别和响应各种难度级别钓鱼邮件的能力，针对薄弱环节开展有针对性的强化培训，补齐短板，从而更好地发挥每一位员工作为反钓鱼“人防”防线的重要作用。

3.游戏化：安全活动运营

通过积分机制激发员工的参与积极性和热情，员工喜闻乐见地接受企业文化和教育，有助于在企业内部形成良好的工作生态，同时竞争排行的机制，更有助于员工激发内生动力，变知识的被动接受者为主动学习者。通过物质或非物质奖励认可员工所发挥的积极作用，让员工真切体会网络安全学习的自我效能感，让安全意识与安全文化在员工中产生情感共鸣。

4.可度量化：测评题库与分析报告

没有量化就没有进步，没有度量就没有效果。通过与宣

传资料及主题培训相配套的题库，较客观地反映出全体员工在安全知识与安全技能方面的差距。通过钓鱼演练分析报告，真实地反映员工识别、防范和响应钓鱼攻击的意识与能力差距。通过设定定量与定性指标，如学习完成率、考试通过率、知识覆盖率、员工触达率、演练中招率、演练上报率、培训满意度等持续性衡量安全意识工作的成效，为下一年项目持续改进提供可量化的决策依据。

（三）关键措施

1.平台工具：自动化安全教育管理平台

项目以自动化安全教育管理平台为主要工具，使网络安全意识教育与钓鱼邮件实战演练相结合，持续为企业数字资产和业务运营安全提供保障。

自动化安全教育管理平台的企业应用学习管理系统具备课程生产、发布、考核、统计等全过程培训管理功能，丰富的学习素材库支撑，同时支持企业自主配置标准/互动课程，可并支持配置各类游戏、竞赛活动类，基于员工角色，推送不同岗位相关的学习内容； 通过平台联动获得员工的风险+学习等各种行为分析，形成积分排名；平台支持个人、部门、企业级仪表看板，支持可定制的统计分析报告。

自动化安全教育管理平台的钓鱼演练系统，通过定期实施模拟钓鱼邮件测试及配套针对性的主题课程推送学习，提升员工识别潜在的安全风险能力，持续开展钓鱼演练可大幅降低员工中招率，改变员工不良风险行为。内置大量基于行业及企业发生的真实钓鱼攻击案例模板，支持 AI 生成钓鱼模版。演练方式包含邮件钓鱼、短信钓鱼、WiFi、U 盘钓鱼。

2.评价方法：人为因素风险与合规度量

网络安全“人、技术、制度”三要素中，技术是核心要素，管理流程是根本，人员教育是关键。但安全意识培训本身并不能降低现实世界网络攻击的风险，员工有了安全意识、知识和技能，并不代表安全团队所期待员工展现的安全行为会自然发生。

“人为因素”安全风险管理是识别、评估和减轻员工因人为因素引发的风险行为的一系列过程，它更关注的行为层面的影响力指标，即行为改变与实际效果。认识到网络安全中“人为因素”安全风险管理的重要性是第一步。项目设定合理的行为度量指标框架，以数据为向导，更准确和直观地衡量员工风险行为的变化。

根据员工的个人风险水平来触发相应的培训和控制措施，充分考虑员工的个体差异，及时识别高风险群体和薄弱环节，基于数据分析为员工量身定制不同的学习路径，提供员工所需的针对性培训，且仅在合适的时间给合适的培训对象提供合适的培训内容，这样可以大大降低传统安全意识培训造成的“培训疲劳”，降低整体培训交付时间和管理成本，也减少了面向低风险群体不必要的培训时间和安全摩擦。

3.持续运营：年度规划、角色化学习

预先设定年度学习、钓鱼演练、知识测评等计划，按照不同的岗位要求设定学习目标。对通用岗位和敏感数据处理活动相关岗位设计不同的安全学习路径，增强员工的学习目标感及学习获得感。通过定期邮件、短信、移动 OA 消息等机制推送学习通知，对持续学习过程与结果进行统计分析。

2022				
序号	主题	电子类		
		图说	动画视频	课件视频
1	邮件安全	备受黑客青睐的钓鱼邮件	电子邮件安全	邮件安全意识培训
2	社会工程	无孔不入的社会工程学	让人防不胜防的社会工程学攻击	社会工程学安全意识培训
3	数据安全	打响数据安全保卫战	数据安全保护	数据安全意识培训
4	个人信息保护	个人信息的泄露与保护	防止信息泄露，乐享网络生活	个人信息保护意识培训
5	合规要求	网络安全法这些你要知道（个人篇）	侵犯公民个人信息有什么后果?	网络安全法执法案例解读
6	密码安全	如何设置安全的密码	密码设置技巧	密码口令保护意识培训
7	差旅安全	差旅安全	差旅安全	企业员工差旅安全意识
8	恶意软件	泛滥成灾的恶意软件	防范恶意软件	恶意软件防护培训
9	办公安全	办公安全两三事	办公环境安全	办公安全意识培训
10	第三方安全	第三方人员安全管理	第三方人员安全管理	第三方人员安全管理
11	移动安全	移动安全问题大爆发	智能手机安全使用	移动设备安全
12	远程办公	远程办公安全指南	远程办公	远程办公网络安全意识培训
2023				
序号	主题	电子类		
		图说	动画视频	课件视频
1	信息安全概念	信息安全的这些知识你知道吗?	信息安全为什么这么重要	全员信息安全意识培训
2	数据隐私	数据隐私，拿什么拯救你?	这份数据隐私保护锦囊请查收!	数据隐私保护
3	终端安全	终端安全，防护指南	终端安全，你我共同守护	终端安全意识
4	网络钓鱼	如何辨别钓鱼仿冒网站	鱼叉钓鱼	网络钓鱼防范意识培训
5	wifi安全	爱恨交织的Wi-Fi	公共wifi安全	wifi安全
6	个人信息保护法	《个人信息保护法》十大亮点	个人信息保护法，这些知识你要知道	《个人信息保护法》解读
7	人是安全要素	人是安全要素	影响网络安全的要素：人为因素	网络安全首要因素——“人”
8	数据保护	涉外数据安全保护须知	守护数据安全	《通用数据保护条例》（GDPR）全解读
9	基础设施保护	关键信息基础设施安全保护条例	关键信息基础设施安全保护条例	《关键信息基础设施安全保护条例》解读
10	勒索软件	揭开勒索软件的真面目	如何防范强势来袭的勒索软件?	勒索软件安全意识培训
11	社交媒体安全	社交媒体安全意识	社交媒体使用中的安全风险与应对	社交媒体安全意识培训
12	物理安全	物理安全	物理安全	物理安全意识培训

图 2-2 2022-2023 年度持续学习情况汇总

（四）系统架构

本项目使用自动化安全教育管理平台的系统功能架构如下图所示：

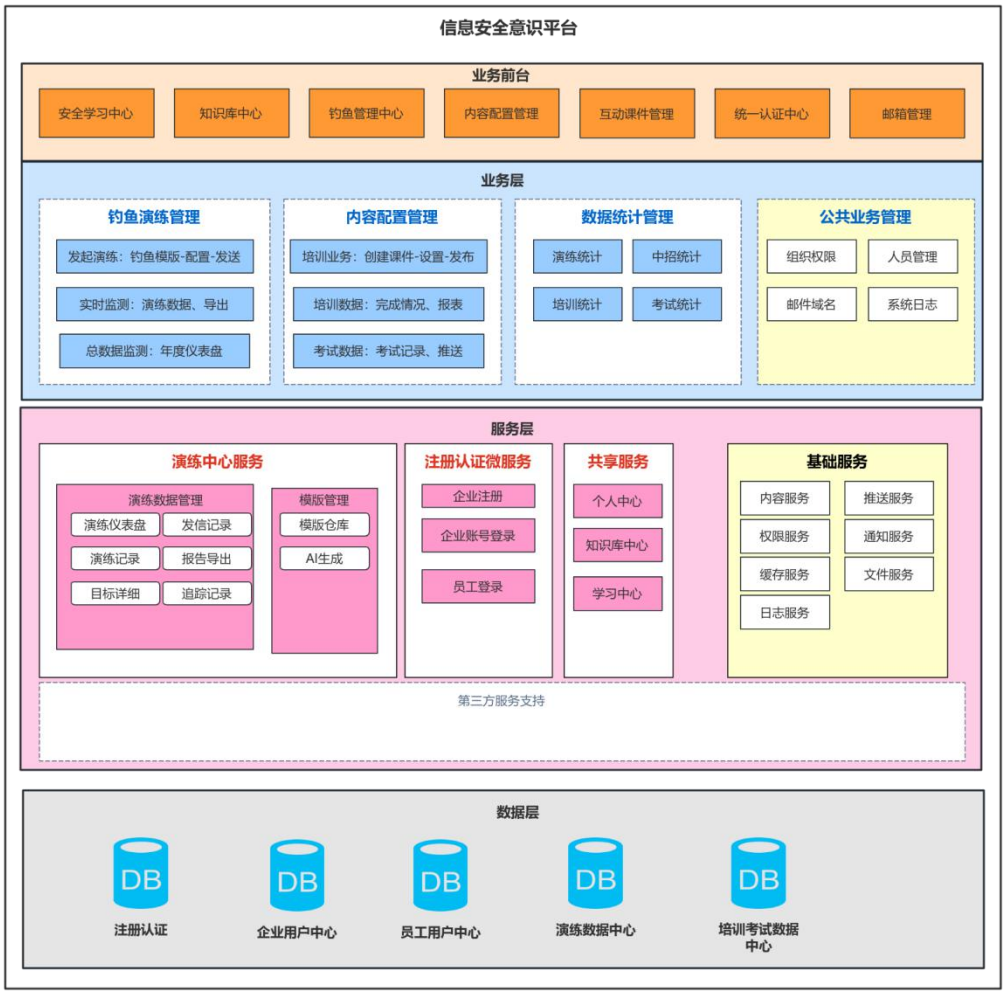

图 2-3 平台系统架构图

用户层内部有企业应用学习管理系统（Learning Management System，以下简称“LMS”）和钓鱼演练两个系统，用户层通过消息组件发送邮件、短信，与第三方即时消息平台对接。

管理层在用户层之下，对内收集用户的学习记录，对用户态度、知识和行为等进行分析；对外收集黑客攻击、漏洞等威胁情报，对部门组织安全状态进行评估，得到针对该员工的个人、岗位、职责、部门、组织等安全意识方面的评估报告。管理层基于上述报告，通过 API 及其他服务自动生成和推送安全意识方面的个性化服务内容，实现员工安全意识

与安全行为的良性循环。

运维层在管理层之下，负责为上层提供负载、网关、缓存、数据存储等基础服务。

（五）管理流程

开展基于钓鱼演练的安全意识培训按以下流程过程进行实施：

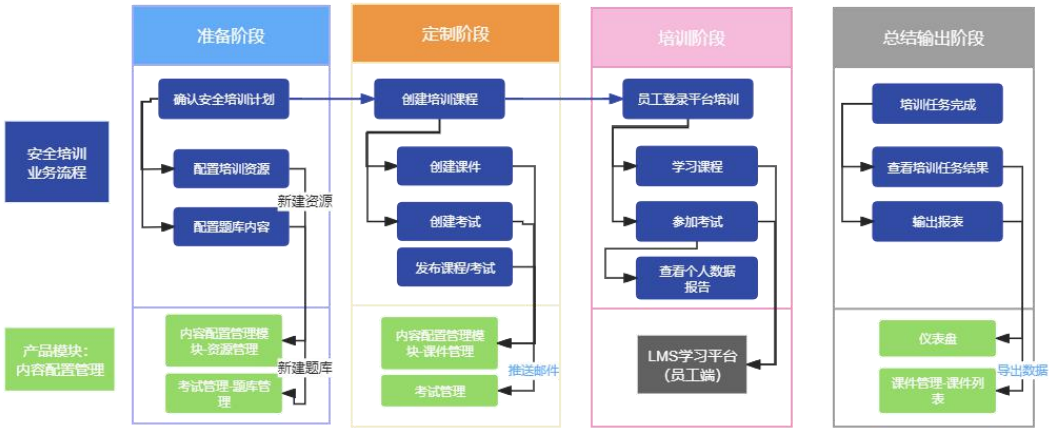

图 2-4 培训计划流程图

1. 安全培训流程：培训管理员通过 LMS 内置的培训主题课程、考试题库，对不同岗位、不同层级的员工进行分组分批次培训，定期推送学习课程，平台对员工学习行为、测试成绩、完成情况形成完整记录。

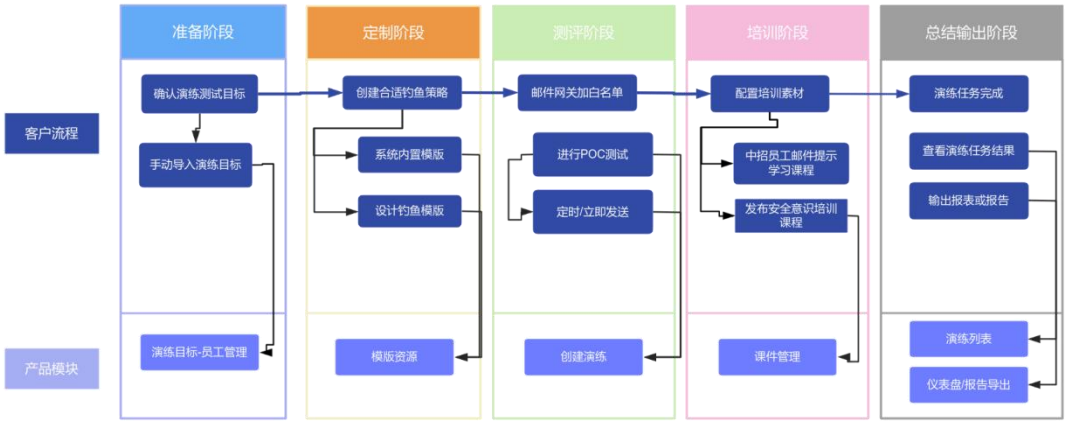

图 2-5 演练计划流程图

2.钓鱼演练流程：企业管理员先确认演练的发送目标，制定演练计划，在平台上实施钓鱼邮件测试服务，设计钓鱼演练模版场景，制定演练发送策略，执行钓鱼演练。在演练测试过程中，可以通过系统实时监测员工的交互行为，对本场演练数据进行分析。测试完成后，通过系统展示和导出测试数据和测试报告，后续根据演练结果针对培训与改进。

（六）技术手段

1.结合行为记录与数据分析技术

针对每位学习者都能提供“私人定制”的学习路线、“千人千面”的学习内容。借助人机交互手段使教学情景更生动鲜活；形式上结合大数据对学习者开展个性化指导，提供精准学习路径，重点补足薄弱环节发展自身优势。

改变目前传统学习状态，针对不同层次的学习者适配教学内容，推送针对性的学习任务及设置合理目标，将教学重点放在问题处置和学习引导方面，促进学习者不断提高学习效率，树立正确的学习态度和认知。

2.支持 xAPI 行为数据接口标准

xAPI 提供了一个以学习者为中心的采集学习行为数据模型，特别是对多数据来源系统的学习记录数据的支持，摆脱了完全依靠单一 LMS 平台的学习记录采集的传统模式，可以跟踪跨平台和跨设备的学习行为，如断开或偶尔连上网络的环境、在任何设备、来自任何服务器、外部网络浏览器等，特别适合对移动学习和互联网学习的支持。xAPI 作为一种用来记录和访问学习行为的技术标准，实现了多平台的学习行

为数据兼容。

3.支持 LRS 学习行为记录

LRS（Local Restore System，以下简称“LRS”）是存储学习行为记录大数据的数据库，LRS 可作为学习平台的一部分，学习平台可直接利用 LRS 中的学习行为大数据进行业务查询、统计、分析。LRS 也可是独立的、公共的学习行为大数据库，来源广泛的网络学习行为都可进行存储，这样就能实现学习行为的共享。

LRS 间能共享数据，因此学习者和数据能从一个组织传向另一个组织。学习行为记录也能被发送到多个 LRS，用户的学习记录能存储在公司的 LRS,也能记录在自己私人的 LRS。应用系统只要获取 LRS 的授权，便可以从中获取学习行为数据，对学习行为数据进行查询、统计、分析及可视化展现等处理，使数据与接口更易标准化、数据服务更加灵活、更易扩展。

4.应用 WebApp 设计互动课件

WebApp 是基于网页技术开发并实现的，运行于网络和标准浏览器上的应用。WebApp 基于网页技术开发的特点实现了应用的跨系统兼容，保证用户在多样性的移动端系统上学习体验的一致性。技术接受模型是运用理性行为理论，从用户体验角度研究系统被用户接受提出的模型。应用 WebApp 设计互动课件，解决跨平台的界面和操作一致性问题，且不需要针对不同客户端进行开发，开发难度小、时间短都利于学习应用的推广。

三、实践成效

（一）思想引领

项目通过 LMS 将各类学习素材进行组织和统一管理，同一素材内容划归为一个主题，将各类素材串联起来形成完整的学习课程，并配套相应题目检验学习成果。

2023 年度，民生加银基金管理有限公司选取上网安全、开发安全、物联网安全、云安全、数据隐私、软件正版化、供应链安全、个人隐私保护、AI 安全、多因素认证、个人信息保护：从意识到行动、数据安全应知应会等教育主题，面向全体员工开展 12 期网络安全主题学习，参与人次达 1304 人次，正式员工参与率达 81.52%，培训考核通过率为 97.66%。

图 2-6 主题学习

（二）行为规范

2023 年度（2023.7-2024.7），民生加银基金管理有限公司安全意识演练共 10 次，累计发送 3100 封邮件，通过仿真常见钓鱼场景，采取威胁风险识别和上报行动，增强整体信息安全风险感知与防御能力。

根据统计结果显示[1]，全国金融业(其他)在演练初级阶段的钓鱼基准测试PFR平均值（既中招率）是22.15%。 经过基线钓鱼->培训->再钓鱼（难度升级）-> 再培训的循环 ，发展至中期阶段为9.79%；后期阶段降至3.79%。 金融业(其他) 年度平均中招率为11.91%。

民生加银基金管理有限公司第一次钓鱼演练（2022.7）中招率为17.36%，2023年度第一次中招率为5.59%，最后一次演习中招率为1.57%，低于同行业后期阶段水平。 年度平均中招率为3.52% ，小于同行业年度平均中招率。

整体来说，企业在经过多次安全意识教育，使得企业员工对于网络安全的防范得到提升，也充分反映安全意识在其中的重要性。

（三）文化培育

企业的网络安全教育，是和企业的企业文化、管理文化相一致的，有一种持续改进的机制。将网络安全文化融入到安全生产文化之中，员工接受起来就自然而然。

稳健，源于敬畏。心存敬畏之心，方能稳健而行。网络安全意识教育和钓鱼邮件演练是提升民生加银基金管理有限公司安全文化的重要手段，它们可以帮助员工认识到网络安全的重要性，并将对网络安全的敬畏其内化为日常行为的一部分。

图 2-7 培养员工网络安全意识

四、经验启示

网络安全意识教育是一项人、技术与流程缺一不可的系统性工程，是一项需要全体员工共同参与的集体性工程。从员工的网络安全意识觉醒，安全知识与技能提升，到安全行为养成，再到组织网络安全文化塑造，是一项长期任务，需要循序渐进，全员参与，持续运营，久久为功。

参考文献

[1]中国网络空间安全人才教育论坛.2022.《2022 企业邮件钓鱼模拟演练分析报告》