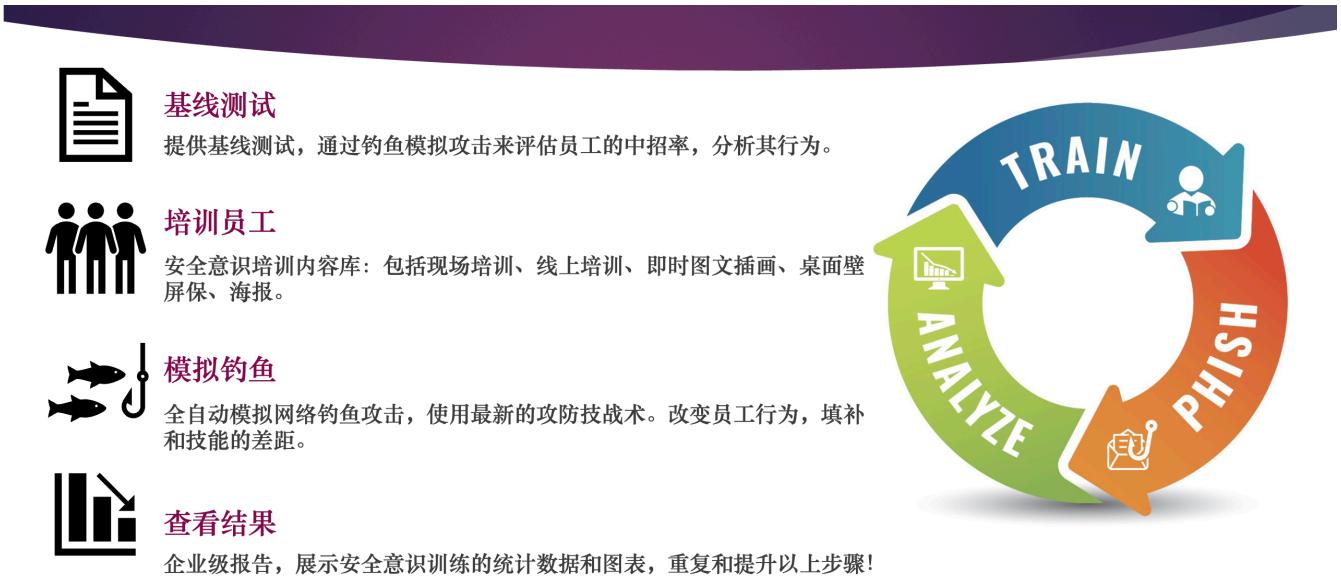
DEEP PHISH

安全意识和反钓鱼训练

服务流程

1 实施过程

总体的实施过程分为四个阶段，如下图。



1.1 第一阶段：基线测试（2 周）

1) 需求调研

收集近年行业相关钓鱼攻击和勒索事件案例，分析企业当前安全弱点，如邮件网关配置、员工点击率等。

2) 制定计划

确定演练场景、工具。 分配角色：攻击组（进行钓鱼投递）、防御组（响应员工报告）、观察组（记录与评估）。

3) 员工宣导

发布安全意识相关通知、邮件提醒、宣传海报等为演练预热，向员工提供基础安全知识手册，如《钓鱼邮件识别指南》。

4) 投递第一轮邮件

准备群发邮件的邮件列表，剔除群组邮箱和敏感 VIP 邮箱地址，投递最低难度的模拟钓鱼邮件（明显伪造的邮件，如拼写错误、非企业域名），评估员工的初始中招率，分析其行为，建立员工安全意识基线。

1.2 第二阶段：培训员工（1 周）

理论培训（线上/线下）

包括钓鱼攻击常用技战术：邮件钓鱼、短信钓鱼（Smishing）、语音钓鱼（Vishing）的识别技巧，

- 发件人地址异常
- 紧急压迫（“立即重置密码”“账户异常”）
- 可疑链接或附件识别
- 案例学习：伪造公司高管邮件要求转账，伪装成 IT 系统要求提供账号密码。

1.3 第三阶段：模拟钓鱼（2 周）

发送两轮模拟钓鱼邮件，逐步提高难度

- 第 1 轮：高度仿真邮件，准备钓鱼邮件主题和内容，模拟 APT 真实攻击编写钓鱼模板，如冒充供应商更新收款账户，"工资条查询"诱导扫码
- 第 2 轮：结合社会工程和心理学技战术，模拟勒索攻击，如最新 AI 生成伪装成“发票”的模拟勒索软件

每轮测试都进行数据记录，如打开率、点击率、数据泄露率、员工上报率和上报时间。 对中招员工进行即时反馈，员工点击链接后则弹出拦截页面，培训钓鱼识别技能和宣导企业安全文化。

1.4 第四阶段：总结与改进（1 周）

1) **生成报告**

统计钓鱼邮件点击率、勒索事件响应时间等数据。 列出高风险部门/个人，针对性强化训练。

2) **制定改进计划**

技术层面：升级邮件网关规则、强化终端安全策略。

管理层面：优化备份策略（如 3-2-1 原则）、完善权限最小化。

3) **定期复训**

每月不定期不通知开展一次反钓鱼训练，确保员工在任何时候遇到钓鱼攻击时尽可能采取正确的行为模式。很多企业都是一年或者半年一次安全意识培训，其实远远不够。对全体员工进行的钓鱼演练，本身也不会起作用。但是，如果把它们放在一起，经常进行，并相互加强，就可以大大提升效果。

2 关键注意事项

1) **安全边界**

全程使用无害的追踪链接或附件，使用无害的模拟勒索软件，确保不会影响真实环境。

2) **法律合规**

模拟攻击在未取得授权的情况下，不得涉及真实用户数据或违法行为。

3) **心理建设**

任务结束后向员工说明结果和管理层的预期，避免员工因“中招”产生挫败感。

3 预期成果

2024 年，整体网络钓鱼中招率平均值为 34.3%，这意味着，未经过培训或未预先通知的钓鱼演练，超过三分之一的员工会中招。在实施安全意识和反钓鱼训练后的 90 天内，这一比例降至 18.9%，通过遵循这些最佳实践，在经过一年的系统化训练后，钓鱼中招率可降低到个位数。

- 通过常态化的训练，可明确降低企业在遭遇钓鱼攻击的失陷概率
- 可验证钓鱼事件上报、失陷主机隔离、数据恢复的标准流程有效性如何，提升跨部门联合共同抵御网络攻击时的协作效率。
- 通过系统化训练和演练，可显著降低企业因钓鱼攻击和勒索软件导致的业务中断与经济损失。

该建议方案通过社会工程学设计训练场景，结合 PDCA 循环实现持续改进，可根据组织规模弹性调整实施强度。建议每半年进行方案迭代，保持与新型威胁技战法同步演进。

训练有素的文化：训练有素的人，训练有素的思想，训练有素的行为。

4 服务周期和交付物

工作阶段	工作内容	周期	交付物
第一阶段	基线测试	2 周	基线测试评估报告
第二阶段	培训员工	1 周	安全意识和反钓鱼培训 PPT

工作阶段	工作内容	周期	交付物
第三阶段	模拟钓鱼	2 周	钓鱼演练报告 勒索演练报告
第四阶段	总结与改进	1 周	演练总结报告

5 服务范围

本方案服务对象为 XXX 公司全体员工，我方可提供的技术支持内容如下，具体内容由双方商榷确定：

1) 平台支持

- 提供自主可控的模拟钓鱼平台
- 在客户使用平台的过程中提供技术支持

2) 顾问服务

- 根据行业特点定制钓鱼攻击场景
- 提供海报设计、安全意识培训、演练报告分析等高级咨询服务
- 政策与流程优化，协助客户制定或优化内部网络安全政策，设计钓鱼事件上报与应急处置流程

3) 持续服务

- 定期更新钓鱼攻击模板，紧跟网络攻击态势
- 提供季度/年度复训，确保员工安全意识得到长效提升

- 钓鱼攻击追踪溯源服务，对日常安全运营遇到的真实钓鱼攻击，提供安全分析服务，判断钓鱼攻击的技战术、破坏性、影响力、针对性

通过常态化的反钓鱼训练，可显著降低企业因钓鱼攻击而导致的财务损失、声誉风险和合规纠纷，建议结合技术防护与员工安全意识形成完整防御体系。