卡巴斯基
安全意识

建立网络安全文化
确保企业安全

kaspersky 引领未来

人为操作成主要威胁

人为操作构成了最大的威胁，
平均64 - 86% 的漏洞与之紧密相关。[1]

数据泄露成本高昂

每个组织遭遇一次数据泄露，平均需承担 440 万美元的成本。[2]

法规强化安全意识

法规明确将安全意识纳入合规范畴，多类标准要求或强烈推荐实施安全意识计划保护敏感数据。

安全意识培育成效凸显

卡巴斯基研究表明，超 85% 完成安全意识培训的员工警惕性显著提升，这一积极行为转变有效降低了事件发生风险。

92%
用户会向其他人推荐卡巴斯基安全意识

300 万
员工已顺利完成卡巴斯基培训计划

160+
不同国家的组织使用我们的培训解决案提升员工安全意识

有效降低人为网络风险的做法

依托扎实的网络安全意识与实用的安全技能，在整个组织范围内构建起积极、稳固的网络安全行为文化体系。这有助于减少由人为错误引起的事件数量。解决人为因素的最佳方法是通过结构化培训计划，将与之相关的最新资讯内容与当下先进的学习方法、技术进行深度结合。

卡巴斯基安全意识解决方案

卡巴斯基安全意识可赋能世界各地、各种规模企业提升员工网络素养，有效塑造安全责任共担的企业文化。由于行为的可持续转变需要经历一定时间，我们的策略聚焦于运用多元工具与强化素材搭建持续学习循环体系：涵盖卡巴斯基交互式保护模拟、高管定制培训、自动化安全意识平台以及 IT 在线网络安全课程。

为什么客户选择卡巴斯基安全意识?

提升发现和应对真实威胁的技能和信心

依托卡巴斯基近 30 年沉淀的网络安全专业积淀与实时威胁情报，我们打造了了高度适配的网络安全培训内容。面对新威胁不断涌现，我们的内容持续迭代升级，助力员工时刻都能有效应对。

人人可及的交互式学习

我们的培训运用结构明晰、逻辑连贯的交互式学习法，助力员工将课程内容与日常工作紧密关联，进而提升理解、记忆与实操能力。

持久的行为改变

我们的方法赋能新技能提升，提供长效驱动力，助力学习深度融入组织日常运作。最终实现行为持续改善，安全实践自然内化。

全面参与

从需要高层次且具有可操作性洞察的高管，到亟待实际指导的前线员工，我们均能以适配形式，为各层级受众精准提供所需材料。

1 卡巴斯基人为因素 360 报告，Cybersecurity Ventures，Verizon 数据泄露报告
2 2025 年数据泄露成本报告，IBM

卡巴斯基自动化安全意识平台：构建人工防火墙

卡巴斯基自动化安全意识平台 (ASAP) 是一款在线工具，可提供持续培训。它能够系统性地为员工输送识别与阻断真实攻击媒介所需的技能和知识，提升企业安全防护能力。

卡巴斯基 ASAP 汇聚全球专家智慧打造，切实赋能员工，强化企业业务根基：

- **减少人为事件**以及由此造成的财务和声誉损失
- 通过**满足监管要求**，降低因不合规产生的罚款风险
- 减少管理意识培训所需的时间和精力并**减轻 IT 团队的负担**

卡巴斯基 ASAP 不只是反钓鱼工具，其培训内容对标 MITRE ATT&CK 技术框架，明确员工可协助防范的人为驱动攻击路径。示例包括：

MITRE 技术	威胁	技能与行为后果
T1566 — 网络钓鱼	恶意电子邮件	识别和报告网络钓鱼尝试
T1585 — 建立账户	虚假账户/个人资料	在共享信息之前验证真实身份
T1199 — 受信任关系	利用合作伙伴的信任	学会质疑不寻常的请求
T1091 — 通过可移动介质复制	可移动媒体	理解 USB 上的恶意软件的危险
T1078 — 有效账户	凭证窃取	避免通过社会工程授予访问权限

95%

参训员工学会识别网络钓鱼攻击

20 倍

持续开展员工培训能减少数据泄露事件[1]

ASAP 涵盖的核心主题包括但不限于：

- 电子邮箱
- 密码和帐户
- 网站和互联网
- PC 安全
- 机密数据
- 个人数据
- 物理数据安全
- 通用数据保护条例
- 人工智能和神经网络
- 对高层管理人员的攻击
- 移动设备
- 社交媒体和即时通讯软件
- 供应链攻击
- 工业网络安全
- 银行卡安全和 PCI DSS
- 如何应对事件
- 语音钓鱼

赋能员工，使其与技术防护手段协同构成额外的安全防护层。

开始试用

1 2025 年卡巴斯基自动安全意识平台研究

内容与方法论紧密结合，旨在提升知识留存率并实现技能转化。

专家驱动

课程内容基于近 30 年的网络安全专业经验和科学的能力模型，涵盖多个维度的实战化核心安全技能。

内容多样

通过交互式模块、实战演练、真实案例分析及多场景模拟钓鱼演练，强化学习效果并巩固安全知识。

丰富的自定义配置选项

支持添加企业商标、品牌证书，并可利用内部课件、制度策略或自定义 SCORM/PDF 模块进一步丰富课程内容，同时支持灵活调整考核结构。

以人为本

基于信息吸收、巩固与应用的认知规律进行设计。

运作机制

网络安全意识应覆盖全员，但知识深度需根据岗位职能及所面临的风险特征进行差异化配置，摒弃“一刀切”的培训模式。我们的平台通过以下核心组件，协助团队构建 500 多项实用技能，实现高效员工分组，并为每位参与者分配匹配的培训方案。

主课

通过依据复杂程度有序组织的微观课程模块，使学习者能够循序渐进地掌握深入知识。

快速课程

快速满足网络安全培训合规标准，通过精炼且富有吸引力的音视频培训内容，及时更新网络安全知识体系。

网络钓鱼模拟器

在培训开展前、进行中以及结束后，分别运行模拟网络钓鱼攻击，全面测试员工抵御网络攻击的实际能力。

课程计划

通过多样化的活动模块，**最大限度提升知识留存率。**

适配各规模组织的易用型方案

便捷的部署流程

在线注册即可获取演示权限，支持多达 5 名用户进行为期两个月的深度体验。提供“入门指南”及在线技术支持

全自动化

培训模块、测试和网络钓鱼模拟会自动分配，与培训组设置一致。

主动式人为风险管理

与卡巴斯基 SIEM、XDR 以及第三方 API 集成，提供员工行为视图。管理员可直接从控制台出发，基于真实安全事件精准分配培训任务。

支持多租户模式与灵活的权限管理

专为拥有子公司或分布式团队的组织设计，在实现总部集中监管的同时，支持将管理权限下放至分支机构管理员。

基于预设规则实现自动化分组

支持按岗位职能、所属部门或风险特征进行灵活组织。

可视化合规报告

仪表板实时展示核心数据，支持深入查看每位员工的进度、延迟或薄弱项，并可一键生成面向管理层的 PDF 汇总报告。

部署灵活

可作为 SaaS 平台或本地安装

快速注册

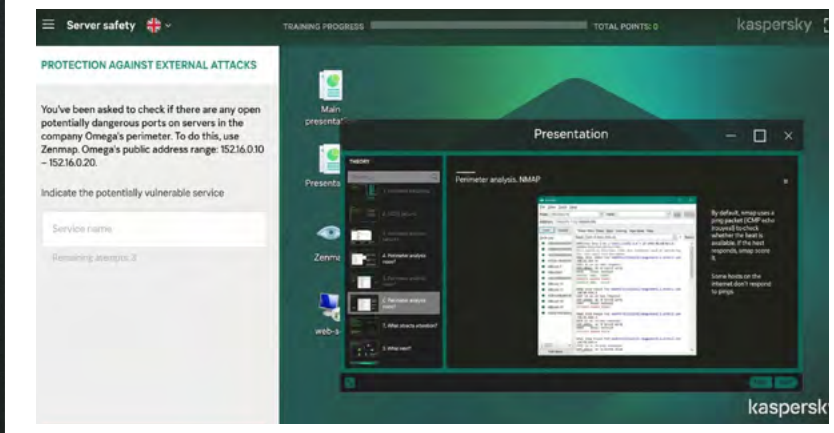
与 Active Directory 和 SSO 集成

IT 在线网络安全

IT 在线网络安全互动培训计划（CITO），专为服务台专员、系统管理员及非专业 IT 安全团队成员量身打造，助力其掌握实操技能，识别日常 PC 事件中潜藏的网络攻击，高效收集关键数据，筑牢网络安全首道防线。

一级事件响应的实用技能：

- 学习检测、分析和响应恶意软件、潜在骚扰程序、漏洞利用和网络钓鱼攻击
- 应用现实世界的工具和技术来加强 IT 基础设施安全并有效调查事件
- 提升日志分析、数字取证及威胁调查的实战技能
- 学习通过强化、策略配置和监视来保护服务器和Active Directory



参与者将通过六大模块展开学习，各模块巧妙融合精炼理论与实用技巧。每个模块均设有 4 至 13 个练习，着重聚焦现实场景中的 IT 安全工具应用与日常任务实践。

恶意软件	潜在有害的程序和漏洞利用	服务器安全
调查基础	网络钓鱼和开源情报	Active Directory 安全

卡巴斯基高管培训

以直观呈现高管决策对风险状况、合规性及长期组织弹性的直接影响为切入点，自上而下营造浓厚安全文化氛围，提升企业安全效能。

卡巴斯基高管培训专为业务领导者及高级管理人员量身打造，以现场研讨会形式开展。培训聚焦当下威胁态势，深度剖析其对企业业务的潜在影响，详细阐释遭遇网络攻击时的应对策略。除传授网络安全核心原则外，更助力参与者洞察安全投资的财务可行性，让 C 级领导者能够精准地将安全防护举措与业务绩效提升紧密关联，为企业稳健发展保驾护航。理想情况下应将此培训与 KIPS 相结合。

以清晰易懂的语言，阐释网络安全中与核心业务紧密关联的关键要点：

- 了解网络安全是整体系统不可或缺的组成部分
- 了解网络风险对业务运营的潜在影响，以及如何管理这些风险
- 了解高级管理层在网络安全治理体系中的核心作用

卡巴斯基交互式保护模拟 (KIPS)：立足企业视角审视网络安全

KIPS 旨在深化管理层对 IT 系统及业务流程中潜在风险与挑战的认知。这是一款专为高级管理人员、业务专家及 IT 资深人士设计的两小时沉浸式团队推演。通过行业特定场景，参与者将面对卡巴斯基专家在实战中监测到的现代攻击手段，如供应链攻击、第三方访问权限滥用、社会工程学及恶意软件等。在有限的时间与预算约束下，团队需制定防御策略、预判安全事件影响并做出有效响应，从而确保业务绩效与营收安全。

促成决策层达成安全共识

实现网络安全风险的可视化，并将其与业务营收及运营表现直接挂钩。

带动全员关注网络安全，构建“安全先行”的企业文化

KIPS 线下版

形式灵活，既可作为独立活动开展，也可作为现有会议、研讨会或企业活动中的一个环节。

- 支持多达 100 人参与，每组 4 至 5 人。
- 配备资深现场讲师及培训助理。

KIPS 线上版

在线版本非常适合全球组织或公共活动。它还可以与 KIPS Live 相结合，将远程团队纳入现场活动。

- 多达 300 个团队（1000 名参与者），地点不限

KIPS 个性化定制选项

- 支持联合品牌或企业专属品牌的推演看板、操作卡片及席位卡定制
- 与卡巴斯基合作构建专属场景，模拟您的网络环境、历史安全事件或特定行业的典型威胁

提供 14 个行业特定场景（持续动态更新）

- 机场
- 公司
- 银行
- 石油与天然气
- 运输
- 发电站
- 水厂
- 地方行政部门
- 石化行业
- 石油控股
- 中小型企业
- 电信
- 技术归因
- IT

构建网络安全文化

网络韧性并非单纯依赖制度与技术，更源于文化文化的重塑取决于个体的行为习惯、管理层的决策导向、流程的设计逻辑，以及技术对全局的赋能，这包括：

· 人与行为　· 领导力与协同合作　· 运营整合　· 安全赋能与就绪能力

可持续的网络安全文化源于持续投入与长期践行。因此，我们构建了一套基于五个关键步骤的体系化方法，并可在各阶段结合卡巴斯基安全意识解决方案加以实施。

贵组织目前的网络安全文化成熟度水平是多少?

0 碎片化阶段
风险：缺乏基础实践与体系支撑，整体安全防护水平较弱。即使是轻微事件，也可能引发严重后果。

1 意识与响应阶段
风险：安全实践主要依赖明确规定的规则执行。在非标准情境下，员工往往依赖个人判断开展操作。

2 托管阶段
风险：事件数量正在减少，但系统仍然容易受到更复杂情况的影响。

3 集成阶段
风险：流程运行看似良好，但若网络安全文化尚未形成自我调节机制，仍存在一定的滞后风险。

4 韧性阶段
结果：事件的数量和严重程度持续下降。企业组织可以快速适应不断演变的威胁环境。

将人员、流程和技术与卡巴斯基 ASAP体系对齐，逐步构建具备网络韧性的安全文化。

立即试用

当安全不再是阶段性举措，而成为组织文化的一部分时，风险将随之降低，成效亦逐步显现。

首席信息安全官

客户参与服务

卡巴斯基
安全意识

了解更多

www.kaspersky.com.cn

#卡巴斯基
#网络安全对业务至关重要