KnowBe4

安全意识培训与网络钓鱼模拟平台

助您成功应对层出不穷的**社会工程**问题

KnowBe4 安全意识培训

老式的安全意识培训已经落伍了。如今，精明狡诈的网络钓鱼和勒索软件攻击常常威胁着您的员工。

基准测试

我们为您提供基准测试，通过免费的模拟网络钓鱼攻击，评估您的用户的 Phish-prone™ 百分比。

培训用户

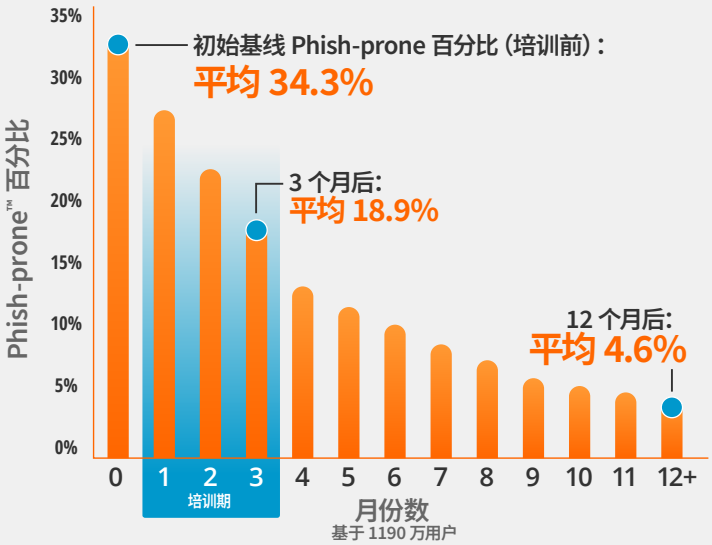
全球最大的安全意识培训内容库，包括互动模块、视频、游戏、海报和新闻刊物。定期发送电子邮件提醒，实现培训活动的自动化管理。

向用户发起模拟网络钓鱼

行业顶级的全自动模拟网络钓鱼攻击、数以千计的无限使用模板及社区网络钓鱼模板。

查看成绩

生成企业防护能力报告，展示培训与网络钓鱼的统计数据和图表，为管理工作做好准备。展现绝佳的投资回报率 (ROI)!



效果显著的培训系统

借助 KnowBe4 的庞大数据库，我们分析了至少 12 个月期间超过 1190 万用户的数据。直至 2024 年，我们的研究仍然反映着令人不安的结果。行业总体的初始 Phish-prone 百分比基准提高至 34.3%，比 2023 年上升了一个百分点。

幸运的是，数据也显示，在部署了新式安全意识培训的 90 天内，34.3% 的比例可降低至 18.9%。这一年的结果显示，通过遵循最佳实践，最终的 Phish-prone 百分比平均可以降低到 4.6%。

快来看看您企业的 Phish-prone 百分比与同行的对比结果吧！您的订阅已含有行业基准测试功能。

资料来源：2024 年 KnowBe4 网络钓鱼行业基准测试报告
注意：初始 Phish-prone 百分比根据所有用户评估结果计算得出。进行评估之前，这些用户没有接受过 KnowBe4 控制台的任何培训。一段时间之后，对已接受 KnowBe4 控制台培训的用户进行评估，得出用户子集的 Phish-prone 百分比。

KnowBe4 安全意识培训功能

无限使用

我们通过 KnowBe4 ModStore 提供 3 个培训访问等级，您可根据订阅等级访问我们的内容库（含 1300 多个项目）。许可灵活，无限访问所有网络钓鱼功能。定期添加强大的新功能。

本地化管理员控制台和学员实践

您可设定三种本地化设置的默认语言：网络钓鱼、培训和管理员控制台语言。通过这三种本地化设置，您的管理员能够选用一种语言（共十种）来管理 KnowBe4 控制台，同时，您的学员还能体验超过 35 种语言的沉浸式培训实践。

内容管理器

借助内容管理器，即可轻松自定义培训内容偏好。调整及格分数，融入品牌化的主题，允许测试，告别内容跳过功能。适用于所有订阅等级。

品牌化的内容

该功能为自助型功能，可让您在选定的 KnowBe4 培训模块的开头和末尾添加品牌定制内容。您可以添加组织的品牌化元素，包括徽标、个性化图案和企业配色，从而量身定制您想传达给用户的信息。

上传专属内容

想要使用您的组织的定制培训或其他企业培训内容来补充您的 KnowBe4 安全意识培训内容吗？借助 KnowBe4 的强大学习管理系统 (LMS)，您可上传兼容 SCORM 的专属培训和视频内容，与您的 KnowBe4 ModStore 培训内容一起管理，无需额外的花费！

评估

了解您的用户所具备的安全知识和安全文化水平，有利于建立基准安全指标。运用技能类评估和安全文化调查，评估和监控您的用户在不同时期的安全知识和安全文化观念。

定制网络钓鱼模板和登陆页

除了上千种易于使用的系统模板以外，您还可根据个人信息定制相应场景并添加模拟附件，以创建专属的针对性鱼叉式网络钓鱼活动。每个网络钓鱼电子邮件模板均含有单独的定制登陆页，以便针对未掌握的知识点进行培训。

Phish Alert Button

KnowBe4 的 Phish Alert 插件按钮可让您的用户安全地将威胁电子邮件转发给安全团队进行分析，并从用户的收件箱删除对应电子邮件，以防未来风险。一次点击，一劳永逸！

社交工程迹象

我们的专利技术将每一封模拟网络钓鱼电子邮件转化为 IT 人员可用的动态培训工具，向员工即时展示邮件中被忽略的危险信号。

人工智能 (AI) 驱动的网络钓鱼和培训建议

利用 AI 的强大功能，为您的用户提供更个性化的体验，以便适应他们的当前知识水平。运用 AI 驱动的网络钓鱼，根据每个用户过往的个人培训和网络钓鱼实践，自动选择最佳网络钓鱼模板。按照 AI 驱动的培训建议，KnowBe4 ModStore 提供针对整个组织的 Phish-prone 百分比的定制培训内容。

用户管理

KnowBe4 的 Active Directory 或 SCIM 集成无需手动管理用户更改，让您轻松上传用户数据并节省时间。根据您的员工行为和用户属性，您可以使用智能组功能来实现网络钓鱼活动、培训评估和补救学习的定制化和自动化。

高级报告功能

60 多种内置报告，为您的关键意识培训指标提供不同时期的整体视图和详细报告。充分利用报告 API，从您的 KnowBe4 控制台中提取数据。此外，通过执行报告，您还可创建并交付定制的执行级别报告。这些报告所提供的洞察可帮助您制定以数据为依据的程序决策。

Virtual Risk Officer™

创新的 Virtual Risk Officer (VRO) 功能利用机器学习，助您预测和识别用户、群组和组织级别的风险。借助这种持续学习模型，有助于您在安全意识计划过程中制定以数据为依据的决策。

回电网络钓鱼

作为一名管理员，您可在 KnowBe4 控制台中使用全新的回电网络钓鱼功能，并开展模拟回电网络钓鱼活动，从而了解您的员工是否会上当受骗。他们的收件箱会收到一封含电话号码和代码的电子邮件。如果他们拨打该号码，就会被要求输入代码。这里的陷阱在于，输入代码属于第一个失败操作，同时也泄露了个人或敏感信息，无疑是双重打击。

PhishER Plus™

PhishER Plus 是一款轻量级的 SOAR 平台，能够对已报告的电子邮件进行自动分析并确定优先级，进而识别和隔离整个组织中的恶意电子邮件。另外，PhishFlip 可将散播的网络钓鱼电子邮件转变为模拟网络钓鱼活动，从而转化为培训机会。

PhishER Plus 增加了经过人工智能验证的众包黑名单和 PhishRIP 功能，能够主动拦截并移除已绕过电子邮件筛选器的活跃网络钓鱼攻击，以免用户遭受入侵。通过减少 SOC 团队所承担的修复工作量，它可节省大量预算和信息安全时间。

您知道吗？88% 的数据泄露是由人为错误造成的。

获取免费的网络钓鱼安全测试，检验您的企业员工的 Phish-prone 百分比

www.KnowBe4.com/PST

KnowBe4 Pte Limited, 80 Robinson Road #02-00, Singapore 068898 | 电话：+65 68132461 | www.KnowBe4.com | 电子邮箱：Sales@KnowBe4.com

© 2023 KnowBe4, Inc. 保留所有权利。本文提及的其他产品和公司名称可能是其各自公司的商标和/或注册商标。

06D06K01