Sophos Phish Threat

缩小最大的攻击面

攻击者始终将企业作为垃圾邮件、网络钓鱼和进阶社交工程攻击的目标，41% 的 IT 专业人员至少每天报告网络钓鱼攻击。您的最终用户通常是容易得手的目标，是网络防御中最薄弱的环节。通过 Sophos Phish Threat 的有效网络钓鱼模拟、自动训练和综合报告，保持用户和企业的安全。

最薄弱的环节的安全与信息安全息息相关

钓鱼式攻击是一门大生意。近年来攻击增长创下新高，现在 66% 的恶意软件通过恶意电子邮件附件安装，而高级针对性网络钓鱼攻击为企业带来平均 140,000 美元/事件的成本。用户依旧是大多数企业的网络安全防御中最容易的攻击者目标，但经过训练的具有网络钓鱼意识的员工可以充当抵御此类威胁的有效防火人墙。

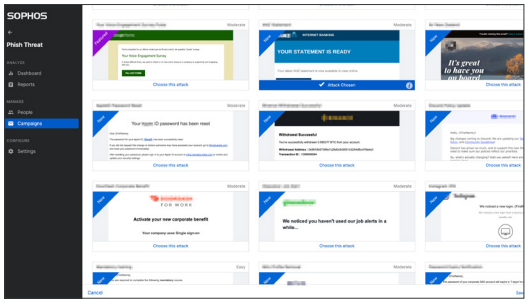
Sophos Phish Threat 模拟一系列网络钓鱼攻击类型，帮助您找出企业安全中的弱点区域，允许用户通过训练强化您的企业防御。

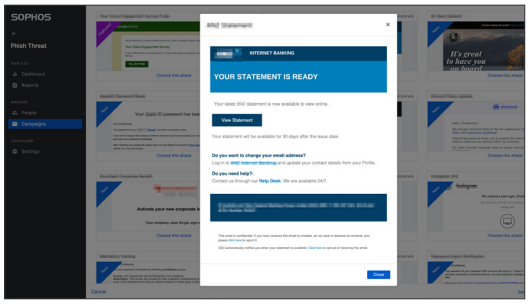
最新的模拟活动

只需单击数次，模拟超过 140 种贴近现实而高难度网络钓鱼攻击。

在 Sophos，我们的全球 SophosLabs 分析师每天监测数以百万的电子邮件、URL、文件和其他数据点，寻找最新威胁。持续的情报流确保用户训练涵盖当前网络钓鱼战术，通过社交相关攻击模拟模板，涵盖多种场景并翻译为 9 种语言:

- 英语
- 德语
- 法语
- 意大利语
- 西班牙语
- 葡萄牙语
- 韩语
- 日语
- 繁体中文





获取不断扩大的国际模板库，从初学者到专家

产品亮点

- 由最新全球网络威胁情报支持的超过 140 个贴近现实而高难度模拟攻击
- 模拟攻击的终端用户个人化培训
- 自动的网络钓鱼攻击报告和培训结果
- 9 种语言选择
- 选择国际托管区域（美国、爱尔兰、德国）

SOPHOS

有效的培训模块

超过 30 个互动式训练模块将教育用户特定威胁，如可疑电子邮件、凭据收割、密码强度和法规合规性。提供 9 种语言选择，最终用户将发现训练具有充分信息和趣味性；面对未来的现实攻击，您可安心：

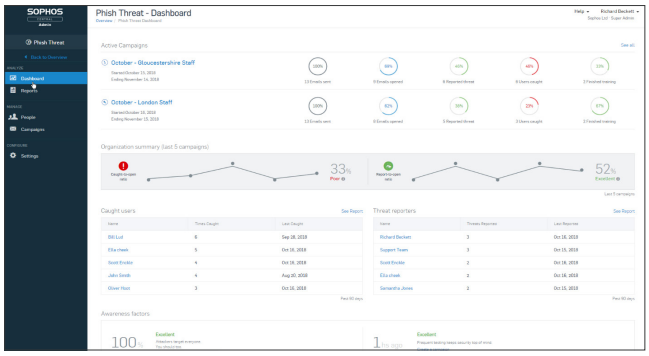
利用精选互动式训练模块吸引用户

全面的报告发送

利用按需的直观仪表板结果，了解企业的安全健康，证明真实投资回报。Phish Threat 仪表板提供关于用户易受攻击性的活动结果概览，允许您用实时意识系数数据衡量整个用户组的整体风险等级，包括：

- 当前用户易受攻击性等级
- 测试的总用户
- 上当的总用户
- 上次活动后的天数
- 平均训练合格分数

深入报告提供企业或单个用户级的更深入信息，带来对企业安全的全新了解。



互动式报告衡量整体风险水平和用户表现

Phish Threat 是 Sophos Central 的一部分

Phish Threat 为基于云的统一安全控制台 Sophos Central 的一部分，通过一个仪表板让整个 IT 部门存取。这意味着无需安装硬件或软件，您可以从实现统一管理网络钓鱼模拟和用户训练，以及电子邮件、端点、移动安全的唯一解决方案获益。您获得一个简单而直观的最新 Sophos 平台。访问 sophos.cn/central 了解更多

轻松启用

Sophos Phish Threat 完全在 Web 浏览器中运行，非常方便。要确保成功投递 Phish Threat 电子邮件，只需将 Sophos Central 控制台提供的 IP 地址，以及 Phish Threat 活动中使用的电子邮件地址和域加入白名单。然后通过 CSV 文件或使用方便的 Active Directory 同步工具轻松导入用户名单。上载用户后，您即可发出第一个活动。

购买软件

每用户的定价在 1 到 5000+ 之间，Sophos Phish Threat 的单一授权许可类型可简化操作，每用户可使用无限量测试，这样您可以将重心放在保护您的用户和企业防御现代高级网络钓鱼攻击上。

免费试用 30 天

访问 sophos.cn/phish-threat，
注册免费 100 用户评估版。

中国销售 (北京)
电话: 400 650 6598
电子邮件: salescn@sophos.com

中国销售 (上海)
电话: +86 21 3251 7160
电子邮件: salescn@sophos.com

中国销售 (广州)
电话: +86 136 0241 6506
电子邮件: salescn@sophos.com

22-11-21 DS-ZHCN (PC)

SOPHOS