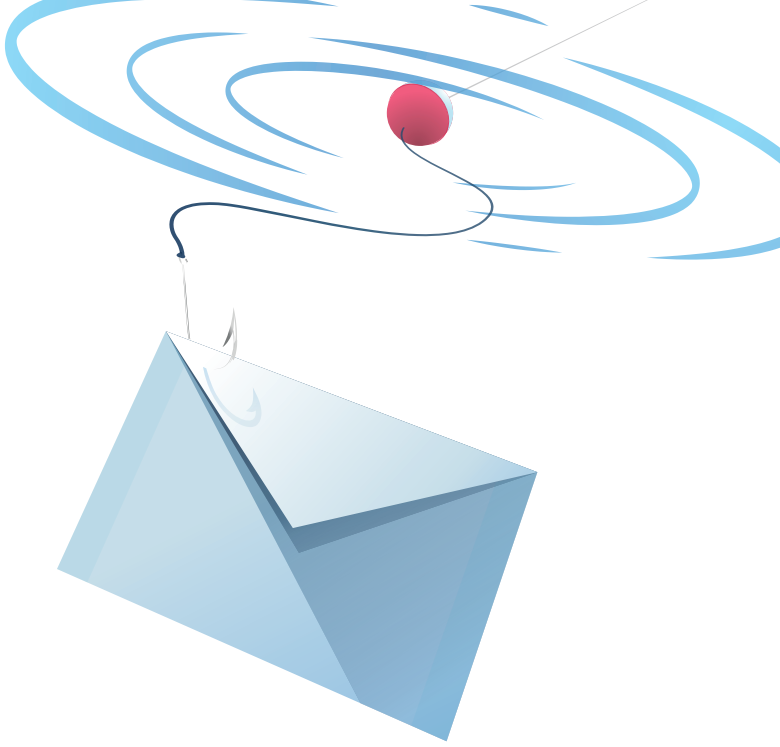
SOPHOS
Security made simple.



勿受骗上钓

网络钓鱼是一门大生意。不要上钩。

在过去一年中，随着攻击者继续改进战术并共享成功的攻击手法，网络钓鱼攻击的数量已经大大增加。尤其是它们使用了深层网络 (dark web) 上的恶意软件即服务功能，以提升攻击的效率和数量。事实上，91% 的网络攻击及后续的数据泄露都是从一封鱼叉式网络钓鱼电子邮件开始的。

在本文中，我们将深入探讨近年来网络钓鱼的发展，以及它的运作方式以及特征。此外，随着网络犯罪分子利用技术继续攻击员工，我们将会强调一个多层次防御网络钓鱼攻击的重要性：将先进的安全技术与受过训练并具备网络钓鱼感知能力的员工结合起来。

不只是烦人的垃圾邮件

我们经常将网络钓鱼视为与网络银行相关的诈骗：诈骗者发送一封电子邮件诱使您造访某网站，但它实际上是仿造银行登录页面的假网站。您若在该假网站上输入自己的凭证，就会掉入犯罪分子的圈套中。

但网络钓鱼不仅涉及假的银行网站，而且还包括健康补充药或包裹送递：它真的如在您面前悬挂诱饵，等待您上钩并为他们提供有用和有价值的信息。

91%
的网络攻击都是从一封鱼叉式网络钓鱼电子邮件开始

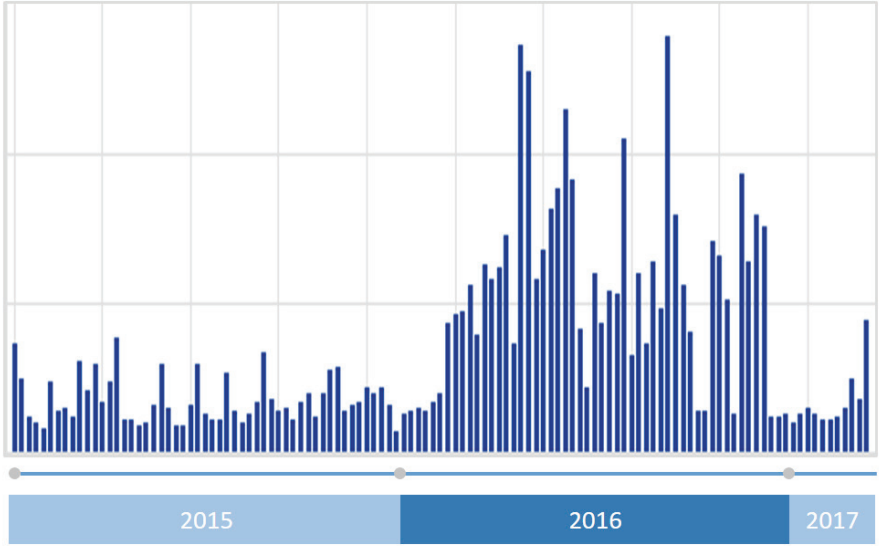
网络钓鱼是一门大生意

在 2016 年，攻击数量大幅增加了，这是因为如免费的网络钓鱼套件和网络钓鱼即服务等来自深层网络的服务所造成的。即使最没有技术能力的攻击者，也能越来越容易地利用其他高阶技术者所产生的高级恶意软件。因此，2016 年被称为「勒索软件元年」(year of ransomware)。

在搭配使用相关内容的诱因时，网络钓鱼活动通常会更容易成功。此外在 2013 年至 2015 年期间，网络钓鱼攻击的趋势都遵循着一致和可预测的模式。在这三年间的每一个时期，网络钓鱼攻击数量每个月都增加，然后在第四季的假期季节时达到高峰。

不过，2016 年并非如此。网络钓鱼攻击的高峰并非出现在年底，而是在今年年中，利用地区特定的事件或恐惧和焦虑期发出攻击，创造出局部性的高峰。例如，2016 年 5 月和 6 月期间，英国脱欧 (Brexit) 投票的不确定性就被用来攻击政府部门。而在美国的税收季节，假借美国国税局 (IRS) 名义的攻击比前几年增加了 400%。

电子邮件威胁 2015 - 2017 年



在 2016 年，攻击的数量大幅增加了，这是因为如免费的网络钓鱼套件和网络钓鱼即服务等深层网络 (dark web) 的服务所造成的，因此被称为「勒索软件元年」。

提高效率和生产率

大多数网络犯罪分子对钱有兴趣。他们若非使用赎金或透过社交工程向您勒索，就是窃取您的数据和凭证并销售到深层网络市场。随着网络钓鱼威胁的演变，攻击者也是如此。

89%
的网络钓鱼是有组织的犯罪

目前，89% 的网络钓鱼攻击是有组织的犯罪行为。由于网络钓鱼已经成为一门生意，攻击策略已经以我们能够识别的方式发展：如何使我的工作更容易且更有效地、我如何逐步扩展业务以增加利润？

因此，更有效的攻击手法出现了，包括随需网络钓鱼服务、现成的网络钓鱼套件，以及新一波的攻击类型，如透过社交工程寻找高价资产的商务电子邮件诈骗 (BEC)。

免费网络钓鱼套件

曾经想让您的产品像新 iPhone 一样热卖吗？对于大多数人来说，如果我们从朋友、同事或竞争对手看到一个成功的做法，就会试图「参考」一下，是吧？在网络钓鱼这个领域也是一样的。其实，它们组织得更好。

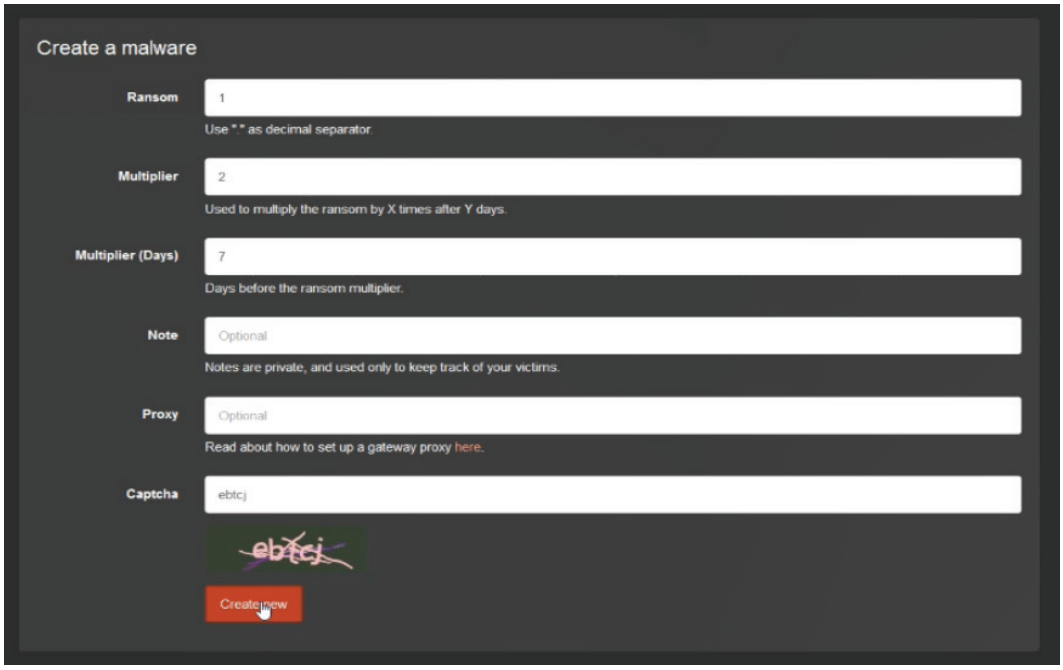
网络钓鱼生态系统有趣的一面是虽然攻击者非常多，但只有少数人有能力从头开始撰写一个网络钓鱼套件。为此，网络钓鱼套件现在大多可以从深层网络的论坛和市场上下载，并为攻击者提供所需的所有工具以进行有利可图的网络钓鱼攻击：电子邮件、网页程序代码、图片等。

套件作者将这些套件分发给其他较弱技术背景的用户，并透过以下两种方式获利：提供免费套件，但其中包含后门，可供作者收集发送者收集的任何数据；或是出售整个套件来获利。现在价格最高的套件甚至包含如活动追踪控制面板等功能。

攻击即服务

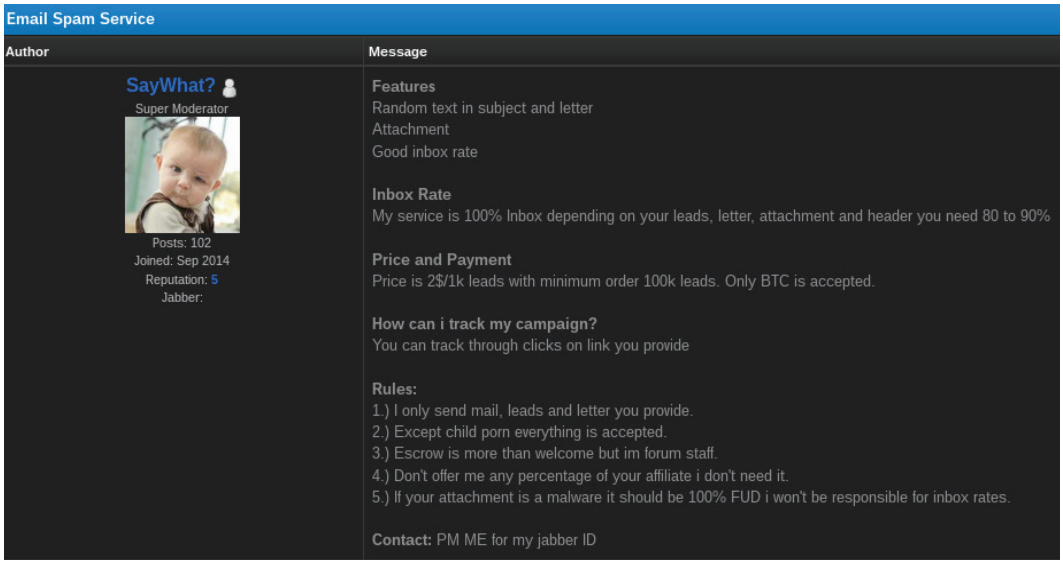
事实上，攻击者甚至不再需要知道如何产生恶意软件或发送电子邮件。现在大多数在线服务技术都是采用即服务 (as-a-service) 和即付即用 (pay-as-you-go) 类型的解决方案，网络钓鱼也是一样 — 攻击者提供越来越多的一系列服务：

- **勒索软件即服务** — 用户只需建立一个在线账户并填写一张简短的网络表格，其中包括起始赎金价格和受害者的延迟付款价格。然后，服务提供商就会从每一笔支付的赎金抽成。如果用户能够将恶意软件程序代码翻译成新的语言或攻击量超过一定等级，则还会提供折扣。



Satan 勒索软件 — 一个在线服务，可让骗徒在几分钟内就产生自己的病毒并开始感染 Windows 系统。

- **网络钓鱼即服务** — 允许用户付钱来发送网络钓鱼攻击，使用全球殭尸网络来避免已知的 IP 躲避范围。甚至保证只对送达的电子邮件收费，就像任何合法的电子邮件营销服务一样。



垃圾邮件发送服务范例 — 每封电子邮件送达到有效收件匣[包含追踪甚至是提供点击率]的价格。

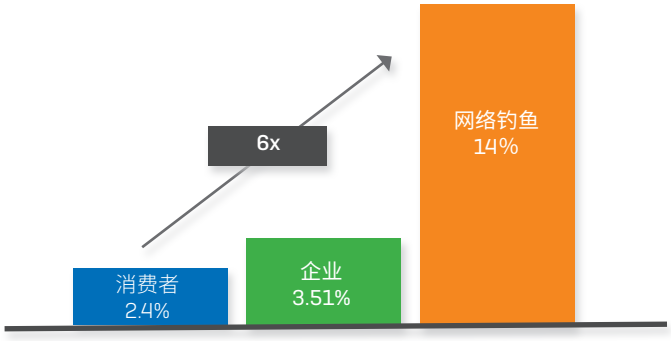
这些服务导致网络钓鱼攻击呈现爆炸式成长（如前所提），因为无论技术能力如何，任何攻击者都可以发动攻击。

仿如营销电子邮件，只是效果好了 6 倍

最令人担心的是，这些深层网络服务能帮攻击者省去大量时间，因此他们可以专注于改进他们的手法并精进邪恶的技能。

而且，他们获得的结果绝对会让大部分销售和营销团队嫉妒不已，因为网络钓鱼电子邮件的点击率比普通的消费者营销电子邮件高出 6 倍。

这个新的研究发现加上发展时间快，使得网络钓鱼威胁更上一个等级。现在，我们开始看到商务电子邮件诈骗（EBC）攻击。这是网络钓鱼攻击的一种危险的新类型，让攻击者能够锁定高价值的企业目标来扩大利润。



网络钓鱼邮件点击率。

来源：Verizon 2016 DBIR & Experian 电子邮件效能测试报告，2016 年第四季

网络钓鱼的运作原理

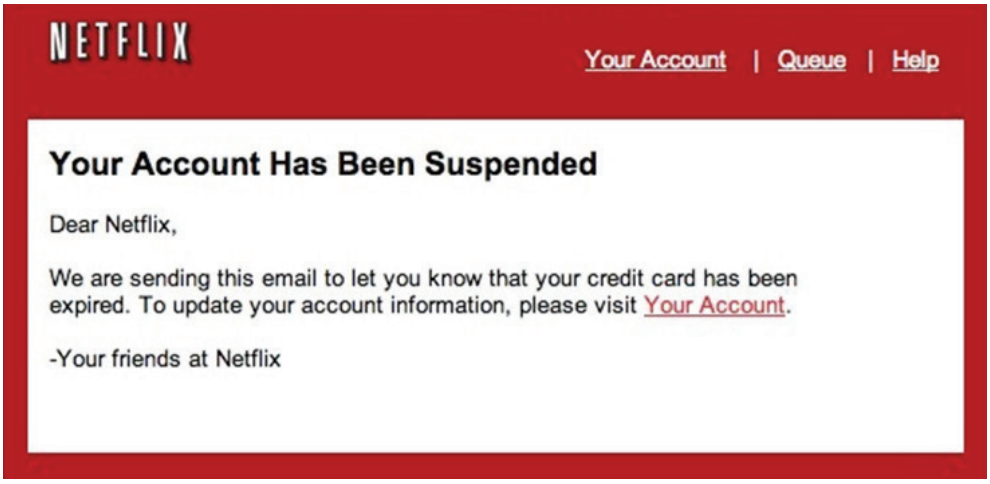
如上所述，网络钓鱼不仅涉及假银行电子邮件和递送包裹的通知。还会说服您为攻击者提供有价值的东西。简单的「网络钓鱼」现在已经发展成为三大攻击类型：经典型、大规模网络钓鱼和鱼叉式钓鱼，以及最近出现的商务电子邮件诈骗（是鱼叉式钓鱼的一种类型）。

31 亿美元在 2016 年 BEC 攻击造成的损失

大规模网络钓鱼

这些攻击主要采取机会主义，利用公司的品牌名称来试图吸引该品牌的客户到假的网站，然后诈骗他们的信用卡信息、登入凭证和其他个人信息，以后再转售以牟利。

- 锁定个人资产
- 通常是消费性品牌的产品或服务
- 大量发送到非特定对象
- 重点在窃取个人数据，如登入凭证

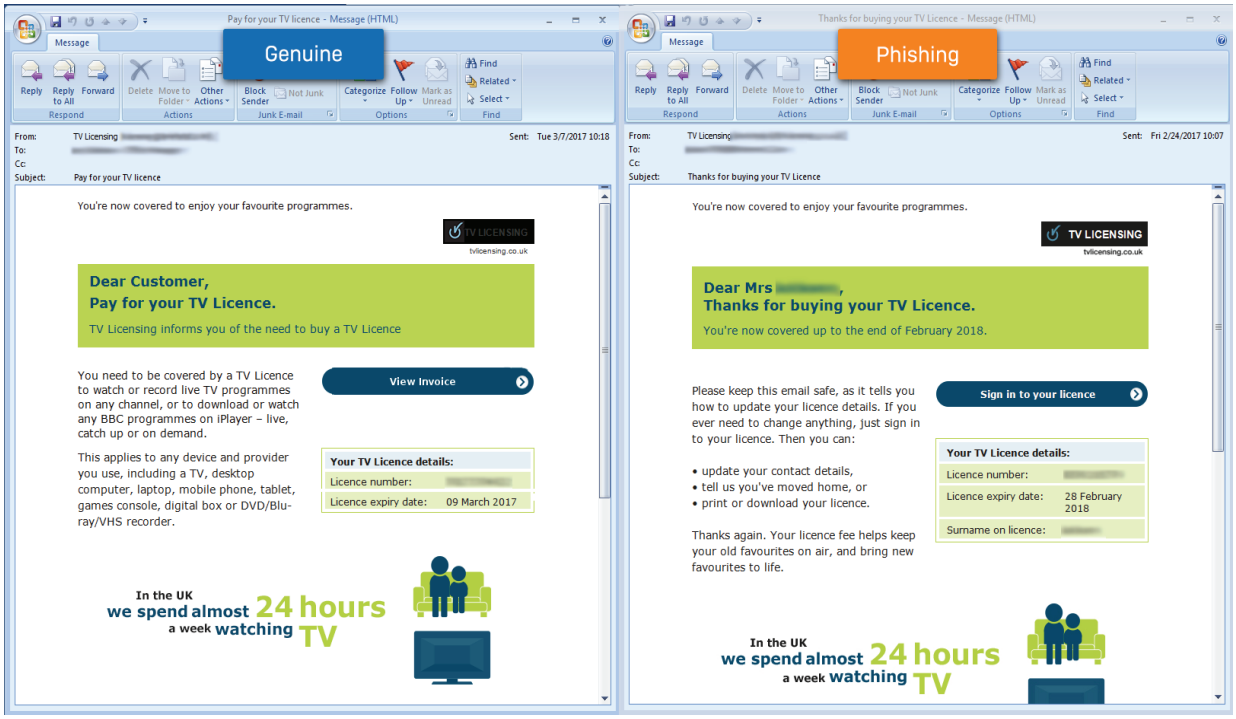


一个典型「验证帐户」的大规模网络钓鱼范例

鱼叉式网络钓鱼

另一种威胁是鱼叉式网络钓鱼。这种攻击会假借特定发件人或可信任来源，发送电子邮件给组织内特定的个人，以试图让他们采取某些移动，例如将钱汇入到假账户。

- 锁定特定组织的资产
- 通常是组织中的个人或特定群组
- 假的（看似真的）电子邮件地址，以协助进行诈骗
- 模仿可信任的来源和高阶管理人员



合法和网络钓鱼邮件通常非常相似，如这个英国电视授权的范例所示。

甚至更具针对性的鱼叉式网络钓鱼手法也出现了，利用社交工程技术来收集目标数据并提高成功率。如众所周知的执行长诈骗 (CEO Fraud)、鲸钓 (Whaling)，以及商务电子邮件诈骗 (BEC) 等。

商务电子邮件诈骗

商务电子邮件诈骗攻击的名称顾名思义，因为它们是与被入侵的员工电子邮件帐户有关的诈骗，而不是假发件人。这使得用户更难以发现攻击。

14 萬美元
每次诈骗的平均损失

- 锁定并骗取公司的信息、存取凭证或是资金
- 在攻击者锁定一个组织后，他们会透过从 Facebook 和 LinkedIn 等网站收集数据来找出该企业中的个人信息，以建构出高度针对性和可信任的网络钓鱼邮件
- 然后，攻击者会让电子邮件看起来是来自高阶主管的讯息，并且会施加时间压力 (通常在一天或一周结束时发送邮件) 来隔离该个人

与大量发送或钓鱼网络活动不同，这些攻击通常是锁定公司资金而来。与前几年透过 PDF 附件对受害者提供汇款银行帐户信息不同，BEC 攻击不会发送这种信息，直到受害者做出积极的响应。毕竟，一个诈骗用的账户将是攻击者在攻击时最大的开销。所以如果受害者早一点意识到这种情况，那么可以将这个重要的信息提供给监管机构。

BEC 攻击更难发现，因为攻击者会入侵企业电子邮件帐户来发送邮件。事实上，最新的联邦调查局的数据显示，数量多得令人震惊的企业堕入这些攻击的陷阱，2016 年受影响的企业达 22,000 家，损失达到 31 亿美元。

找出征兆

所以，若您收到包含假发票的邮件，告诉您有人用您的信用卡买了一张机票，所以请打开附件以便观看付款的详细信息。这就是大规模网络钓鱼。

30%
的网络钓鱼邮件已被开启

还有那些假的快递通知，说他们需要您确认公司的地址，以便递送未送达的物品，也是一样的。

大体上来说，鱼叉式网络钓鱼的手法非常雷同，除了诱饵更具体之外。或者，在 BEC 攻击中，该邮件可能不包含恶意链接或附件，而是要求您转账 — 使攻击看起来更可信。

简单地说，如果诈骗电子邮件的一开头是「亲爱的客户」，那就是网络钓鱼。但是，如果该邮件是以您的名字向您致意，那就是鱼叉式网络钓鱼。如果它是来自您老板的实际电子邮件地址，那么就是一个商务电子邮件诈骗 (BEC) 攻击。

当然，许多鱼叉式网络钓鱼攻击比这还更尖锐，如果您可以接受这个比喻的话。处心积虑的骗徒可能会知道您的职务、您的座位号码、您经常造访的三明治店、聊天的朋友、老板的名字、以前老板的名字，甚至公司咖啡提供商的名字。

而且，正如您可以想象的那样，就鱼叉式钓鱼而言，一事顺利，成功接踵而来。骗徒、网络犯罪集团或国家赞助的行动者越了解您的公司，他们的网络钓鱼攻击将会更可信。

可以透过很多方式取得这些信息，包括：

- 以前的成功攻击，如数据窃取恶意软件
- 私人公司文件，例如在搜索引擎中显示的电话簿或组织架构
- 您的个人和公司社交网页
- 心怀不满的离职员工
- 向深层网络上的其他骗徒购买的数据

您可能还会想到很多许多方法来让「秘密」变成不是秘密。底线是，了解这些手法能让您成功地避免打开今日被开信的 30% 网络钓鱼邮件之一。

打击网络钓鱼

网络钓鱼邮件的类型和规模形形色色，但不幸的是，没有一个产品将完全保护您的业务免受网络钓鱼攻击。在打造针对网络钓鱼攻击的多层次防御时，结合先进的安全技术和受过网络钓鱼训练的员工是唯一的答案。

若要获得保护，您需要建立多道防线：

先发制人在门口阻挡威胁	保护您最弱的一环：用户	确保您的最后一道防线
电子邮件和网络保护	**用户培训**	**防漏洞入侵和防勒索软件保护**
• 实时威胁更新 • 阻挡恶意附件、内容和网址 • 防诈骗 • 网址过滤 • 点击时网址保护 • 恶意软件沙盒	• 培训 • 测试 • 报告	• 新一代漏洞入侵防御 • 分析 • 清理
Sophos Email Protection **Sophos Web Protection**	**Sophos Phish Threat**	**Sophos Intercept X**

先发制人在门口阻挡威胁

您防范网络钓鱼攻击和其他电子邮件威胁的第一次机会，就是强大的电子邮件和网页过滤。

电子邮件网关是对网络钓鱼邮件的最佳防御。电子邮件保护是您的守卫，可阻止网关上 99 % 的不想要电子邮件，包括恶意附件、内容和网址，让用户没有机会看到它们。点击时网址保护 (time-of-click) 技术可以避免用户联机到受感染的网站 (即使电子邮件进入收件匣时是干净的)，而云端沙盒也会在远程执行夹带macro附件的电子邮件。

网页过滤是另一个不可或缺的前端防御，可在用户点击电子邮件链接时过滤和阻挡受感染的 URL。而档案沙盒技术会确保从威胁链中及早移除那些令人讨厌的恶意软件下载。

保护您最弱的一环：用户

即使拥有最佳的前端过滤工具，没有任何执行档或连结可侦测的攻击手法 (如 BEC) 有机会逃过侦测。适当的培训和教育，对于确保所有员工知道如何发现和处理这些类型的电子邮件，至关重要。请寻找可以编辑的模拟针对贵组织攻击的方案，还有可让您导出员工表现报告的功能，以便奖励表现良好的员工并协助改善他人的表现。

确保您的最后一道防线

如果心不在焉的用户无意间点击连结，让有效且强大的恶意软件进入系统了，您仍然有足够的机会阻挡破坏，甚至是扭转结果。新一代的入侵程序防御解决方案可以识别、分析和遏止即使是最先进、未曾发现的恶意软件，并会自动清理所有感染的痕迹，让您可以安然度过这一天。

了解您的业务

确保员工了解公司的流程。您应鼓励员工对来自其他员工和高阶管理人员 (无论多么高阶) 的不寻常的请求进行质疑，或许最重要的是确保您会采用两阶段批准流程来处理所有重大的资金转账请求。如没有执行适当查核流程，世界上的所有防御措施都无法阻止员工将大笔款项交给小偷。

Sophos 具有强大的技术，可以在攻击的每个阶段保护您。如需更多信息，请造访 Sophos.com/phishing。

十个网络钓鱼的迹象

这些「迹象」可以让您找出潜在的骗局。

1. **它看起来有问题。**电子邮件讯息中是否某些地方有点奇怪?怎么可能会有这么便宜的事?相信您的直觉。
2. **通用的称谓。**网络钓鱼电子邮件通常会使用「尊敬的客户」等通用称谓,而不是直接指名。这种客观用语可以节省网络犯罪分子的时间。
3. **联机到看似官方外观的网站并要求您输入敏感数据。**这些假网站通常非常有说服力,因此请注意对方要求您透露哪些个人信息或机密数据。
4. **使用您的特定信息的不请自来电子邮件。**只要从如 LinkedIn 等社交网站,就可以收集到如工作职位、过去就业或个人兴趣等信息,并用来制作一个令人信服的网络钓鱼邮件。
5. **令人不安的措辞。**窃贼经常使用令人不安的措辞 (例如说您的账户已经被骇),骗您尽快采取行动且在不经思考下透露您通常不会揭露的信息。
6. **差劲语法或拼字错误。**这通常是一个大破绽。不异常语法也是一个有问题的迹象。
7. **急迫感。**「如果您在 48 小时内没有回复,您的账户将被关闭。」窃贼会透过创造急迫感来希望您犯错。
8. **「您中大奖了!」**这种网络钓鱼邮件很常见,但很好识别。类似,更狡猾的的手法就是要求您完成一项调查 (这您就提供个人信息) 以换取奖品。
9. **「验证您的账户。」**这些邮件伪装成真实的电子邮件,要求您验证您的账户。持续寻找网络钓鱼的迹象,并总是质疑为什么要会被要求验证 — 很有可能这就是一个骗局。
10. **网络蟑螂。**通常,网络犯罪分子会购买并「躲藏」在与官方网站相似的网站名称上,希望用户造访错误的网站,例如 www.google.com 与 www.g00gle.com 。在输入您的个人信息之前,请务必先查看一下 URL。

如需更多阻挡网络钓鱼的提示和工具,请造访 www.sophos.com/prevent-phishing

北京办公室
电话:400 650 6598
电子邮件:salescn@sophos.com

上海办公室
电话:+86 21 3251 7160
电子邮件:salescn@sophos.com

英国牛津

2017-04-03 WP-UK (MP)