简译版

五种方法降低电子邮件假冒攻击风险

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	5 tips to reduce the risk of email impersonation attacks		
原文作者	切坦·阿南德（Chetan Anand）	**原文发布日期**	2020 年 10 月 23 日
作者简介	切坦·阿南德是 Armorblox 公司的架构师。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/10/23/tips-reduce-risk-email-impersonation-attacks/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

五种方法降低电子邮件假冒攻击风险

切坦·阿南德

2020 年 10 月 23 日

多年来，电子邮件攻击已经不再局限于普通的网络钓鱼，变得更具针对性。在本文中，我将重点介绍电子邮件假冒攻击的危险性，并提供一些建议，帮助个人和企业降低遭受此类攻击的风险。

电子邮件假冒攻击是什么？

电子邮件假冒攻击是指，攻击者冒充受信实体，利用恶意电子邮件诱骗受害者，以窃取资金和敏感信息。被冒充的受信实体可能是任何人——老板、同事、供应商，或自动获取其邮件的品牌厂商。

我们通常会对受信实体的邮件快速采取行动，因此此类攻击非常有效且很难捕获。攻击者还配合使用其他技术，来欺诈企业并窃取其账户凭证。有时，受害者在被骗几天后都未能发觉。

幸运的是，我们可以遵循下述安全最佳实践，以降低电子邮件假冒攻击的风险。

1. 寻找社会工程线索

电子邮件假冒攻击依赖于语言，这种语言通常会引起受害者的紧迫感或恐惧感，迫使他们采取攻击者希望的行动。当然，并非每一封带来紧迫感或恐惧感的邮件都是假冒攻击。但是，这是一个值得关注的因素。

以下是假冒邮件中经常出现的短语和情况：

- 要求短时间内转账汇款或提供敏感信息。
- 异常采购要求（例如 iTunes 礼品卡）。
- 员工突然要求更改工资卡信息。
- 供应商共享新产品。

2. 对电子邮件进行情境检查

在针对性电子邮件攻击中，受害者通常很忙，做不到“三思而后行”。我们应花费几秒钟的时间，问问自己，收到的邮件及其要求是否合理。

- 为何 CEO 会要求你在两小时内购买 iTunes 礼品卡？他们以前是否这样要求过？
- 为何 Netflix 邮件会发送到你的公司邮箱？
- 为何 IRS 会通过电子邮件要求你提供 SSN 等敏感个人信息？

总结一下：即使邮件来自受信实体，也要三思而行。

3. 检查邮箱地址和发件人姓名之间的差异

为了防止假冒邮件，很多企业部署了基于关键字的保护措施，筛选邮箱地址或发件人姓名与高管姓名（或其他相关关键字）匹配的邮件。为了绕过这些安全控制措施，假冒攻击使用的邮箱地址和发件人姓名，与所冒充实体的邮箱地址和发件人姓名略有不同。需要注意的一些常见偏差如下：

- 更改拼写，尤其是乍一看不会发现的更改（例如，将姓名中的“ie”改为“ei”）。
- 根据视觉相似性进行更改以欺骗受害者（例如，将“rn”替换为“m”，因为它们看起来很相似）。
- 在无事先通知的情况下，从个人账户（如 Gmail 或 Yahoo）发送企业电子邮件。如果发件人是第一次通过个人账户向你发送邮件，建议通过辅助渠道（消息，Slack 或电话）验证发件人的身份。
- 姓名的描述性更改，即使该更改符合情境。例如，冒充首席技术官瑞安·弗雷泽（Ryan Fraser）的攻击者，发送发件人为“瑞安·弗雷泽，首席技术官”（Ryan Fraser，Chief Technology Officer）的邮件。
- 更改发件人姓名的某些部分（例如，添加或删除中间名首字母，将 Mary Jane 缩写为 MJ）。

4. 了解假冒邮件的常见短语和策略

电子邮件假冒攻击已经存在了很长时间，我们需要认识一些常见短语和策略。假冒邮件

不一定都与资金或数据直接相关——第一封邮件可能是一个简单的请求，只是为了看看谁会上钩。我们需要注意以下短语/情境 ：

- “您现在有时间吗”，“您在办公桌前吗”等问题是假冒邮件中经常出现的开场白。它们只是简单的请求，看似无害邮件，因此能够通过邮件安全控制措施并撒下诱饵。
- “我需要紧急帮助”，“能否在接下来的 15 分钟内帮我个忙”等暗示邮件非常紧急的短语。如果你从“CEO”那里收到这样的邮件，你很可能会迅速做出回应并受骗。
- “您可否告知个人手机号码”，“我需要您的个人邮箱”以及其他有关个人信息的情境外请求。这些要求的目的是收集信息并了解受害者；一旦攻击者掌握了足够的信息，他们就可以假冒受害者了。

5. 使用附加身份鉴别方法

多年来，越来越多的企业开始采用双因子身份鉴别（2FA），这有助于保护员工账户并减少账户泄露的影响。

如果收到涉及资金或数据请求的异常邮件，我们应采用下述最佳实践。

- 供应商是否恰好在应收发票到期时，通过电子邮件向你发送了银行账户信息的更改？致电或发短信给供应商，确认是否是他们发的邮件。
- 经理通过邮件要求你购买礼品卡？向他们发送 Slack 消息（或你使用的任何办公应用）来加以确认。
- HR 代表通过邮件向你发送了 COVID 资源文档，但是要求输入邮箱凭证才能浏览？请与 HR 代表核实邮件是否是他们所发。

即使你需要联系非常忙的人员进行附加身份鉴别，他们也会理解并感激你的谨慎性。

通过上述方法，个人和企业可以更好地了解电子邮件假冒攻击并降低其风险。但是，要想有效防止电子邮件假冒攻击，不能只靠眼睛。企业安全团队应对其电子邮件安全堆栈进行彻底审计，并增强本地电子邮件安全功能，以提供针对假冒邮件的特定保护。

在我们的数字生活中，电子邮件比以往任何时候都更为重要。因此，我们需要确认，发件人就是声称的本人，这一点至关重要。电子邮件假冒攻击正是利用了“冒充”方法。要想阻止此类攻击，我们需要将安全措施、提供假冒防护的电子邮件安全解决方案以及谨慎性（即

使邮件看似来自受信实体，也要保持谨慎）相结合。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com