电脑用户安全意识月刊

OUCH!

本期摘要

- 什么是CEO诈骗?
- 自我保护

CEO诈骗

什么是CEO诈骗?

网络罪犯非常狡猾，他们总是不断想出一些新的攻击手段来达到他们的目的。成功率最高的方法之一就是以你这样的人群为目标。虽然网络攻击者知道缺乏安全意识的人是一个组织里最薄弱的环节，但是他们忘记了像OUCH!读者一样的具有安全知识的人能够成为一个组织的最佳防御机制。

客座主编

Angela Papas是汤森路透集团的信息安全培训与意识的主管，负责大使计划以及对员工进行网络钓鱼的培训。

网络罪犯开发出一种新的攻击方式，即CEO诈骗，也被称为企业电子邮件诈骗。在这种攻击中，网络罪犯冒充自己是目标人群所在企业里的CEO或者其他高级主管，通过向员工发送电子邮件，企图诱导被攻击者做一些不应该做的事情。因为网络罪犯为此做了大量的功课，这种类型的网络攻击成功率非常高。首先，不法分子通过查询企业的官方网站能够获取到诸如地理位置，公司管理层以及合作伙伴等相关信息。其次，再通过LinkedIn， Facebook或者Twitter等社交网络了解到你同事们的个人资料。一旦他们掌握了你的企业组织结构，他们就开始通过进一步的调查从而锁定攻击对象。网络罪犯根据自己的需要有目的的选择攻击对象：如果他们想要获取钱财，可能会以财务部的员工为目标；如果想要获取税务信息，可能会以人力资源部门为目标；如果想要获得数据库服务器的权限，那么可能会以IT部门员工为目标。

一旦网络攻击者确定了他们的犯罪目标和攻击对象，他们就开始着手准备网络攻击。其中最为常用的手段就是鱼叉式网络钓鱼。网络钓鱼是指网络攻击者向成千上万的人群发电子邮件，企图诱导用户上当受骗，比如打开一个受感染的附件或者访问一个有病毒的网站。鱼叉式网络钓鱼是网络钓鱼的一种，区别在于，攻击者并非向大量人群发送邮件，而是向少数的目标群体发送一封内容具体的定制邮件。这些鱼叉式钓

CEO诈骗

鱼邮件看起来非常真实，很难被辨别。它们被伪装成来自你认识的人或者与你共事的人，比如同一个公司的其他员工、甚至是你的老板。这些电子邮件看起来非常逼真，因为它们或许会使用同事之间使用的行话，公司商标或者甚至是一个高管的官方签名。这类的邮件往往会刻意制造一种非常紧急的情势，要求你马上采取行动而且不能够告诉其他人。网络罪犯的目标就是诱导你在仓促中犯错。以下是三种常见情况：

CEO诈骗是一种成功率极高的的网络攻击方式，能够规避大部分安全防御机制。最终，你才是所在企业的最佳防御。

电汇：网络罪犯的目标是钱财。这意味着他们做过调查并且知道谁在财务部门的人员。网络攻击者伪造电子邮件，冒充他们的主管，告诉员工这是一个紧急事件，必须马上给指定账户转账。

税务诈骗：网络罪犯想要盗取你的同事的个人信息用来假冒员工 。他们调查你所在的企业并锁定能够掌握员工信息的人，比如，人力资源部门职员。然后网络罪犯发送伪造的电子邮件，冒充一位高级管理人员或者法律部门的人员，要求马上获得某些文件。

假冒律师：CEO诈骗不总是通过电子邮件进行的，像电话等手段也可能被使用。在这种情况下，网络罪犯一开始先伪装成高级管理者向你发送电子邮件，告知你将会有一位律师给你打电话讨论意见紧急事件。随后他们会冒充律师给你打电话。这些网络罪犯会谈论一些情势紧迫且机密的事情，来制造出一种非常紧张的气氛。这种紧张感很可能会诱导你按照他们的安排做事情。

自我保护

那么，你能够做什么来保护自己以及公司的利益呢？生活常识是你最好的防御手段。如果你收到一条来自老板或者同事的信息，但是听上去怪怪的或者感觉有问题，那么这可能就是一次网络攻击。能够辅助

CEO诈骗

判断网络攻击的线索有：一种巨大的紧迫感、一个看起来有问题的签名、一个不正常的说话方式，或者邮件里使用的名字并不是你同事通常对你的称谓等等。另一条线索是攻击者使用了一个你从来没有见过的电子邮箱地址或者电话号码，也有可能是与你同事或者老板的邮箱地址极为相似却不相同的邮箱。当你心存疑虑，直接给他们打电话或者当面确认（不要通过回复该问题的邮件进行确认）。不要试图规避公司的安全条例或者程序。你的公司或许有明确的规章制度知道你进行转账授权或者发送机密文件的正规流程。所有试图绕过这些流程的要求，都应该被质疑，并且在采取措施之前一定要经过确认。如果你收到了这种要求但是不确定该怎么做，立马告知你的主管，帮助台或者网络安全小组。

了解更多

订阅OUCH!　安全意识月刊，查看OUCH!往期内容，以及了解有关SANS安全意识方案的其他内容，尽在 securingthehuman.sans.org/ouch/archives.

Dyn is a cloud-based Internet Performance company. Dyn helps companies monitor, control, and optimize online infrastructure for an exceptional end-user experience. Through a world-class network and unrivaled, objective intelligence into Internet conditions, Dyn ensures traffic gets delivered faster, safer, and more reliably than ever.

相关资源

社会工程学:	https://securingthehuman.sans.org/ouch/2014#november2014
网络钓鱼:	https://securingthehuman.sans.org//ouch/2015#december2015
家庭网络安全手则:	https://securingthehuman.sans.org/ouch/2016#march2016
二步验证:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip of the Day:	https://www.sans.org/tip-of-the-day

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
翻译：陈柳希