SANS SECURITY AWARENESS

OUCH!

給大家的安全意识通讯月刊

首席执行官欺骗行为/业务电子邮件隐患（BEC）

什么是首席执行官欺骗行为/业务电子邮件隐患（BEC）？

网络攻击者继续发展电子邮件攻击，称为首席执行官欺骗行为，或业务电子邮件隐患（BEC）。 这些带有针对性的电子邮件的攻击，都是诱使受害者作出一些不应该做的行为。 在大多数情况下，这些坏人都是为了金钱而来的。 甚么令攻击变得如此危险，是网络攻击者在发动攻击前会先研究他们的受害者。 而且，安全技术也很难阻止这些攻击，因为没有感染病毒的电子邮件附件或恶意链接监测显示。 这里是攻击的工作原理。

网络攻击者利用互联网来研究他们的目标受害者和受害者互动的人，例如：如果他们瞄准你， 他们会研究谁是工作上的老板，又或是在家里工作時常联系的房地产经纪人。 网络攻击者会制作一封电子邮件，假装是上述人等，然后发送电子邮件给你。 这封邮件非常紧急，要求您立即采取行动，如处理发票、更改付款人、或说服你，令你回复敏感文件。 这封电子邮件目的是迫使你去做他们想要的。 这里有两个例子：说明了这种攻击是如何产生作用。

电汇：网络罪犯是为了金钱。 他们研究你的工作单位，例如找出谁在应付帐款中工作，或者谁负责资金转移。 犯罪分子会制作并傳送一封电子邮件给这些人，去假装是他们的老板或高级执行官。 这电子邮件告诉他们有一个紧急情况，並且必须将钱马上傳到一个新的银行帐户内。 这电子邮件迫使他们犯错，实际上他们在向网络罪犯者傳送资金。

税务诈骗：网络罪犯将人们的个人信息來用于税务诈骗。 其中一个最快获取此项的方法，就是窃取公司所有员工的信息。 网络罪犯研究和鉴定谁在人力资源部工作。 然后他们给这些人发送假邮件，假装成高级主管，或者是司法部的人。 这电子邮件创建出一个紧急的故事，必须把所有员工的税务信息立即提交。 人力资源的人认为他们将敏感文件发送给高级管理人员，而实际上他们将信息发送给网络罪犯。

保护自己

那么你能做些什么来保护自己呢？ 基本常识便是你的最佳防御。 以下是最常见可找出的线索。

这电子邮件是非常短和紧急的 (通常只有几句话) 还有的是签名上显示电子邮件是从移动设备发送的。

这是一种强烈的紧迫感, 迫使你忽视或绕过你雇主的政策。 总是遵循相关的政策和程序, 即使电子邮件看似来自你的老板甚至首席执行官。

电子邮件应是与工作相关的, 但是使用了个人电子邮件地址, 如@gmail.com或@hotmail.com。

电子邮件似乎来自您认识或工作上的资深领导、同事或供应商, 但该邮件的内容方式并不像平时的他们。

提供了付款指示被, 这些指令跟以前收到的不同, 例如要求立即付款去到不同的银行帐户内。

如果你怀疑你在工作上已成为目标, 应停止与攻击者的所有互动, 并给你的主管报告。 如果你是在家里成为目标, 或者你成为受害者同时亦已并进行了电汇, 那便要立即通知你的银行, 然后再向执法部门报告。

特邀编辑

Don Cavender 是一名前联邦调查局 (FBI) 特工, 在数字取证和网络犯罪已有22年以上的丰富经验。 他最近针对网络犯罪组织成为华盛顿的业务电子邮件隐患协调员。 他在数字取证和网络调查方面, 提供培训和进行研究。 @don_cavender https://www.linkedin.com/in/donald-cavender

资源

社会工程学:	https://www.sans.org/u/HE3
停止此网络钓鱼:	https://www.sans.org/u/HE8
停止此恶意软件:	https://www.sans.org/u/HEd
锁定您的登录:	https://www.sans.org/u/HEi