每月安全意识通讯

个性化诈骗

概述

网络罪犯不断想出新的和富有创意的方法来愚弄大众。 一种新型诈骗方式正逐渐流行——个性化诈骗。 网络罪犯找寻或购买数百万人的信息，然后用这些信息来定制他们的攻击。 下面我们将向你展示这类诈骗是如何实施的，并带你看一个常见案例。 你关于这类诈骗了解得越多，你就越能容易地识破并阻断它们。

它是如何进行的？

电子邮件诈骗和电话诈骗并不新鲜，网络罪犯已经企图愚弄人们很多年了。 例子就包括"你中奖了"和著名的尼日利亚王子诈骗。 然而，在这类传统的诈骗中，网络罪犯不知道他们的目标是谁。 他们仅仅是创造一条泛泛的消息，然后将其发送给数百万人。 这类诈骗因为内容很泛，所以通常很容易就能被识破。 个性化诈骗就不同，网络罪犯首先会做调查，然后为每个目标创建一条定制化的消息。 他们通过找寻或购买包含人们名字、密码、电话号码和其它详细信息的数据库来做到这一点。 这类信息很好获得，因为有很多网站都被入侵了。 这类信息也常见于社交网站和公开的政府记录中。 罪犯接着会瞄准他们拥有相关信息的每一个人。

一个网络罪犯常用的伎俩就是使用恐吓或胁迫来迫使你给他们打钱。 这类攻击是这样进行的。 他们找寻或购买从被入侵的网站上泄露的人们的用户名和密码。 他们在这样的一个数据库里发现你的账号信息，然后向你（和数据库里存的其他每个人）发送一封含有你的一些详细信息——包括你在被入侵的网站上用的原始密码——的邮件。 罪犯将你的密码作为入侵你的电脑或设备的"证明"——这当然不是真的。 罪犯然后声称他们不仅入侵了你的电脑，还抓住了你在网上看色情内容。 邮件接着会威胁说，如果你不交封口费，他们将向你的家人和朋友分享关于你的难以启齿的网上活动的证据。

问题是，在几乎所有的类似情况下，网络罪犯根本没有入侵你的系统。 他们甚至不知道你是谁，或是你访问过了哪些网站。 诈骗者仅仅是企图用他们知道的关于你的星星点点的个人信息来吓你，让你相信他们入侵了你的电脑或设备，并且骗你给他们打钱。 记住，坏人也可以将同样的技巧用在电话诈骗上。

我该做什么?

认识到这类电子邮件和电话其实是诈骗。 当某人知道你的个人信息时，你感到害怕是很正常的。 然而记住，发件人在撒谎。 这次攻击是一次大规模自动化行动的一部分，并不是直接针对你的。 如今网络罪犯要找寻或购买个人信息已变得越来越容易了，所以，准备好在未来遇到更多这样的个性化诈骗。 有些线索你可以注意。

⚠

- **任何时候，当你收到十分紧急的电子邮件、消息或电话时，保持高度怀疑。 如果某人运用了恐惧、焦急等情绪，他是在想让你在慌乱中犯错误。**
- **当某人要求你通过比特币、礼品卡或其它不可追踪的方式付款时**
- **当你收到一封可疑邮件时，在 Google 上搜索，看看有没有其他人报告过类似的攻击。**

最终，基本常识便是你的最佳防御。 然而，我们也建议给你的每一个网上账号使用独一无二的长密码。 记不住你所有的密码? 使用密码管理器吧。 此外，尽可能启用两步验证。

特邀编辑

Lenny Zeltser 是一位网络安全领域的老兵。 他在 Minerva Labs 制作反病毒解决方案，并在 SANS Institute 教授安全课程。 他在托管安全服务与咨询方面也有经验。 你可以在 zeltser.com/blog 和 Twitter (@lennyzeltser) 上关注他。.

资源

社会工程学:	https://www.sans.org/u/MUU
有关社交媒体的重要提示:	https://www.sans.org/u/MUZ
搜索引擎运算符:	https://www.sans.org/u/MV4
OSINT 框架:	https://www.sans.org/u/MV9