SANS SECURITY AWARENESS

OUCH!

給大家的安全意识通讯月刊

停止网络钓鱼

概述

电子邮件和通讯服务(如: Skype、Twitter 或 Snapchat)都是我们主要沟通方式之一。 每天我们不仅用这些技术来应付工作,亦可用于与朋友和家人保持联系。 自世界上这么多人依赖着这些技术，它们都成为标网络攻击者使用为主要攻击手段之一。 不论您是在工作还是在家里，都要去了解网络钓鱼到底是什么， 以及如何能够发现和停止这些攻击。

什么是网络钓鱼

网络钓鱼是一种典型的攻击，它使用电子邮件或消息服务来骗您去使用不应采取的操作，例如: 点击恶意链接、共享密码或打开受感染的电子邮件附件。 攻击者会设法去使这些信息更能获得信服和引起你触发情绪， 例如紧迫感或好奇心。 他们可以让他们看起来像他们来自某人或你知道的东西,例如朋友或来受那些你经常使用你所信任的公司。 他们甚至可以把您的银行徽标添加或伪造电邮地址，令信息显得更加合理。 然后攻击者会将这些信息发送给数以百万计的人。 他们不知道谁会上钩，他们只知到，发送越多，便越多人将会成为受害者。

保护自己

几乎在所有的情况下，打开和阅读电子邮件或讯息都是没问题的。 为了进行网络钓鱼攻击，坏人们都会需要欺骗您做一些事情。 幸运的是，有些线索会表明消息是一种攻击。 下面是最常见的原因:

- 有一种巨大的紧迫感,会要求在糟糕的事情未发生之前《立即采取行动》， 比如威胁要关闭帐户或将你送进监狱。 攻击者想催促你犯错误。
- 迫使你绕过或忽略我们的安全程序或政策。
- 有一种强烈的好奇心或有些东西好得令人难以置信。 (不，你并没有赢彩票。)

- 像 "亲爱的客户" 这样的一般称呼。 大多数与你联系的公司或朋友都会知道你的名字。
- 要求提供高度敏感信息，比如你的信用卡或密码，又或者該合法发件人应该已经知道的任何其他信息
- 消息说：它来自一个官方组织，但语法或拼写非常差，或者使用像 @gmail 这样的个人电子邮件地址。
- 邮件是来自一个官方的电子邮件 (例如你的老板)，但有一个回复地址会去到 "某人" 的个人电子邮件帐户。
- 如果你收到一条来自熟人的信息，但是说话语气或信息内容看起来不像他或她 ，如果你怀疑，请打电话给发件人确认消息是否由他们发出。 网络攻击者很容易制造一封看起来像发出來自你朋友或同事的邮件。

最终，基本常识便是你的最佳防御。 如果邮件看起来奇怪、可疑或是内容好到令人难以置信，那么它可能就是網路釣魚攻擊。

特邀编辑

托尼娅-达德利 自2011年以来，她一直在开发和运行安全意识计划，其中包括建设了一个获奖的网络钓鱼培训计划。 搜寻她请登上 www.linkedin.com/in/toniadudley.

资源

Social Engineering:	https://www.sans.org/u/Cb1
Helping Others Secure Themselves:	https://www.sans.org/u/Cb6
Email Do’s and Don’ts:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! 翻译和档案:	https://www.sans.org/u/Cbq

许可证

OUCH! 由SANS Securing The Human出版，并以 Creative Commons BY-NC-ND 4.0 许可证分发。只要您不修改内容，您可以随意分发本通讯，或者将其用于您的安全意识项目。有关翻译或更多信息，请联系 www.sans.org/security-awareness/ouch-newsletter. 编委会: Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley | 翻译：李贵娟