电脑用户安全意识月刊

OUCH!

本期摘要

网络钓鱼

概述

电子邮件作为人们交流的一种主要方式，不仅被广泛用于日常工作，还是我们与亲朋好友联系的桥梁。除此之外，大多数公司通过电子邮件提供在线服务，比如确认网购交易或者提供银行对账单。全世界人们对电子邮件的依赖性，也使其成为网络犯罪的主要攻击方式之一。我们将在本期简报中解释一种常见的电子邮件攻击方式——网络钓鱼，以及如何安全使用电子邮件。

客座主编

Lance Hayden博士，Berkeley Research Group的常务董事，是一位安全文化和行为的专家，其著作People-Centric Security: Transforming Your Enterprise Security Culture由麦格劳-希尔集团出版。更多信息：www.linkedin.com/in/drhayden。

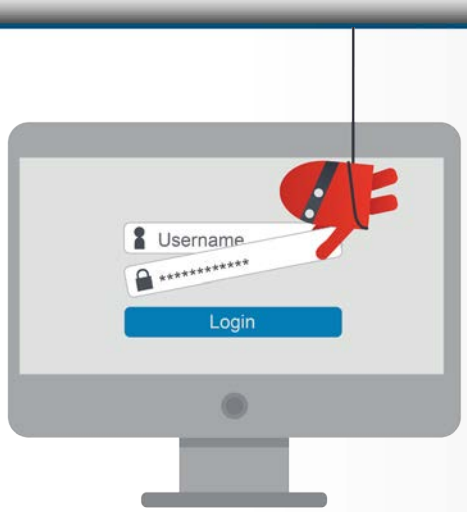
网络钓鱼

网络钓鱼是指利用电子邮件或者信息服务诱骗用户采取某种行动（如点击社交网站上的一个链接或者打开一个附件）的一种网络攻击方式。受骗用户会面临敏感信息泄露或者电脑中毒的危险。攻击者不择手段地将钓鱼邮件做的很有说服力。比如，他们会把假的电子邮件做的看起来发自你知道的一些人或者机构，例如你的朋友或者你经常使用的一个可信的公司。攻击者甚至会在电子邮件中加入银行商标或者把发件人的电子邮件地址伪造的更合法。然后攻击者把这些邮件发给成千上万的人。他们并不知道谁会上当，他们只知道发出去的越多，有人上当的可能性就会越高。网络钓鱼，顾名思义就是撒网捕鱼，你并不知道你能不能捞到鱼，但是撒的网越大，你捞到的鱼就会越多。以下是几种常见的网络钓鱼攻击的方式。

- **获取信息**：攻击者的目标是获取你的个人信息，比如密码、信用卡号或者银行信息。因此，攻击者的邮件会包含一个链接，点击链接会跳转到一个看上去正当的网站。该网站会要求你提供你的账号信息或者个人资料。然而，这个网站是个假的，你输入的所有个人信息都会直接落入攻击者的手中。
- **恶意链接**：攻击者的目标是控制你的个人设备。当你点击来自攻击者邮件内的链接，你会打开一个发送攻击的网站。一旦成功，你的设备系统就会被入侵。

网络钓鱼

- **恶意附件**：同样的，攻击者的目标是入侵并控制你的个人设备。有别于前一种方式，攻击者会直接通过邮件发给你一个被感染的文件，比如一个Word文档。打开该文档会触发攻击，有可能会使得攻击者控制你的系统 。
- **骗局**：有些钓鱼邮件无非是骗子使用电子邮件进行诈骗。他们的骗术包括告诉你你中奖了，伪装成慈善组织进行募捐，或者寻求你的帮助来转移一大笔金额。如果你回复了他们的邮件，他们会向你索取服务费或者要求进入你的银行账户，从而骗走你的钱。



生活常识是你的最佳防御手段。如果一封电子邮件或者一个信息看起来很古怪，很可疑，或者内容看起来是天上掉馅饼，那它很可能就是钓鱼攻击。

自我防范

在绝大多数案例中，仅仅打开并且阅读邮件或信息是安全的。钓鱼攻击者需要诱导你做进一步的行为才有可能得逞。幸运的是我们可以判断出来一个信息是否是钓鱼攻击。下面列举了最常见的几种判断方法：

- 该邮件企图营造出一种紧张气氛，要求你需要“立即采取措施”来阻止一些不好的事的发生，比如你的账户即将被关闭。攻击者试图利用人在紧急情况下不能够理性思考的弱点从而诱导用户上当受骗。
- 你收到的邮件包含莫名其妙的附件或者该邮件极力怂恿你打开附件。比如一封邮件声称附件里是公司尚未宣布的裁员名单，员工工资信息或者一封国税局的起诉信。
- 该邮件不直接称呼你的姓名，而是用一个非常笼统的称呼，比如“亲爱的顾客” 。大多数联系你的公司或者朋友应该知道你的姓名（用户名）。
- 该邮件向你索取高度敏感信息，比如你的信用卡号或者密码。
- 该邮件声称来自一个官方机构，但是有病句、错别字，或者来自个人邮箱地址，比如@gmail.com，@qq.com，或者@163.com。
- 邮件里的链接地址看起来很奇怪或者不像官方链接。一个方法是把鼠标悬停在该链接上直到浮动窗口出现，悬浮窗口上显示才是该链接真正的地址。如果邮件里的链接地址跟浮动窗口的地

网络钓鱼

址不一致，不要点击。在移动设备上，长按该链接可以看到同样的浮动窗口。一个更安全的方法是粘贴邮件里的链接，然后复制到你的浏览器地址栏或者直接在浏览器输入正确的地址。

- 你收到的信息是来自你认识的人，但是说话的口吻和措辞并不像他或者她本人。如果你有疑虑，直接打电话给发件人进行确认。网络攻击者可以轻而易举地写一封看上去来自你的朋友或者同事的邮件。

如果你认为一封电子邮件或者信息是钓鱼攻击，直接删掉它。基本上你的生活常识就是最好的防御方法。

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http://www.securingthehuman.org.

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://www.securingthehuman.org/ouch/2014#november2014
保证安全的五个步骤:	https://www.securingthehuman.org/ouch/2014#october2014
我被入侵了，怎么办?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS 每日安全妙招:	https://www.sans.org/tip_of_the_day.php

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

