如何快速识别网络钓鱼信息

作者：庄艳

如果您拥有自己的业务，例如会计、网络营销、咨询公司等等，虽然您不一定和顾客直接见面，但您的生意可能会受到另一种来自网络安全的威胁。您是否为自己的业务购买了适当的保险呢?

很容易识别的网络钓鱼，并且仅限于电子邮件形式的日子已经一去不复返了。虽然恶意消息并不是什么新鲜事，但它们正变得越来越复杂，并且越来越难以从合法的商业通信中辨别出来。他们还通过短信、社交媒体、聊天甚至电话来找我们。

什么是网络钓鱼?

网络钓鱼是一种恶意活动，在这种活动中，诈骗分子试图获取对用户信息、数据或设备的访问权限。目标是让您在无暇思考的情况下采取行动，当您这样做时，网络钓鱼者可能会：

- 获得他们可以利用的数据和信息。
- 在您的系统上安装恶意软件。
- 引导您透露您的个人财务信息，以窃取金钱或您的身份。
- 访问您的电子邮件并向您的联系人发送其他恶意邮件，以诈骗他人。

企业是否特别容易受到网络钓鱼的攻击?

是的。随着越来越多的工作以数字方式进行，各种规模的企业都容易受到攻击。攻击者还假设小型企业不会在其安全措施上花费大量金钱或精力，从而使它们成为潜在的更容易攻击的目标。

网络钓鱼者可以很容易地在网上找到您的联系信息，并且相信他们发送给您的消息至少会被查看，因为您从事的是快速响应客户的业务。网络钓鱼邮件也变得越来越复杂，因此您很容易被说服访问恶意网站，或下载看似合法的邮件中的受感染文件。如果他们碰巧是给您打电话的网络钓鱼者，他们会非常有说服力地让您按照他们的详细说明向他们提供您的宝贵信息，或安装他们的恶意软件。

如何发现网络钓鱼攻击?

写得不好、向您提供大量金钱，或要求您提供经济援助的网络钓鱼邮件长期以来一直很普遍。我们大多数人都知道不要打开、点击或回复这些消息。如上所述，网络钓鱼尝试也不限于电子邮件。黑客现在使用您的手机号码等电话号码给您打电话，并试图让您透露敏感信息。他们也可能会向您发送短信。

最近，网络钓鱼邮件被设计成看起来像您可能收到的其他电子邮件。它们可能看起来是来自您信任的人，例如银行、朋友、软件提供商、零售商或供应商，但通常，消息的发送时间是出乎意料的。

例如，一种常见的技术是黑客通过网络钓鱼尝试获得对电子邮件账户的访问权限，然后访问该账户并使用恶意链接回复真实的电子邮件对话。因此，当收件人收到这封电子邮件时，它看起来像是先前对话的延续，但它要求收件人下载文档或输入他们的密码凭据。

如何防止网络钓鱼攻击?

在您、您的员工、客户和其他一般消费者之间的日常业务过程中，您应该熟悉您的正常营业活动。如果您收到意想不到的消息、电话或电子邮件，甚至看起来有点不对劲，请在采取行动之前验证消息的有效性。打电话给发送该消息的人，询问他或她是否发送了消息。如果答案是否定的，那就是恶意消息。

您可以做的其他事情：

1、尽可能多地启用多重身份验证(MFA)服务，例如您的电子邮件。如果您碰巧中了网络钓鱼者的一个诡计，拥有这一额外的保护层将大大有助于减少他们接管您的电子邮件或其他目标帐户的机会 。

2、使您的软件和设备保持最新状态。Microsoft Office产品、操作系统、第三方应用程序（例如Adobe Reader）和智能手机操作系统的最新更新包含可防止最新安全问题的补丁。

3、将光标悬停在电子邮件中的链接上以显示URL。如果它看起来可疑，请不要点击它。

4、在您的设备上使用现代端点保护软件。它们通常由McAfee和Norton等常见和知名安全品牌提供。Microsoft 还为 Windows 和其他应用程序提供端点保护。

5、始终备份您的数据，以便在您成为攻击的受害者时尽快恢复业务。定期测试您的备份过程以确保它们按预期工作。

6、对您的员工进行网络安全实践教育，例如如何识别网络钓鱼企图和垃圾邮件。根据世界经济论坛的说法，高达95%的网络安全问题都可以追溯到人为错误——因此员工教育很重要。

7、查看Microsoft Word附件上的扩展名。大多数用户已经更新了他们的Microsoft产品，以便Word文档以.docx结尾。如果您看到过时的.doc扩展名，请慎重。

8、此外请注意，如果您受到攻击，您可能不会立即知道，第一个迹象可能是您的客户收到了您的意外邮件。不幸的是，直到客户可能打电话来验证您发送的内容时，您才知道自己受到了攻击。

如果客户打电话询问消息是否合法，在您确认是否发送了该电子邮件后，请向他们提供您在自己的业务运营中使用的相同的规范操作。

客户是否预期收到该电子邮件？链接或URL是否指向合法的预期网站地址？它是否要求他们打开他们没有预料到的可疑文件？它是否要求他们提供用户ID和密码，威胁要剥夺或禁用他们的访问权限?

回答这些问题可以帮助您确定邮件是否安全。

随着犯罪者采用新的技术和形式，网络钓鱼也在不断变化和发展，因此必须制定良好的安全计划并注意新出现的攻击，以帮助保护您的业务。一个训练有素的团队知道如何发现可疑消息，也可以很好地防御网络钓鱼攻击。

庄 艳（专业保险经纪人）
微信：ReliableInsurance
邮箱：Yan@reinso.com
电话：765-464-0384

为您的企业提供的正确的保护

联系值得信赖的保险顾问，了解一些保护您的业务的明智且负担得起的方法。例如，ERIE等保险公司提供的Cyber Suite可以帮助您解决客户或员工的非公开个人信息如果遭到泄露，而您必须将泄露事件通知他们的情况。您可以将这一项保险背书添加到您的商业保险单中。