网络保险：保护小型企业免受社交工程欺诈

作者：庄艳

为什么中小企业成为目标?

如果您是一家小企业主，为什么犯罪分子会针对您而不是收入更高的知名企业呢？根据小企业管理局的数据，小企业占美国国内生产总值的44%，犯罪分子针对小企业的攻击有其合理的理由，包括：

安全预算低。较小的公司往往有较少的安全预算。通常，由于没有专门的安全团队或缺乏最新的对策，它们比预算更充裕的大公司更容易成为目标。

安全协议薄弱。与规模较大的公司相比，规模较小的公司更有可能采用不太成熟的安全策略和协议，从而导致敏感信息得不到重视和保护。

通往更大猎物的门户。通过实施供应链攻击（利用为众多大客户提供服务的小公司的漏洞），攻击者通常可以通过同时非法访问多个受害者来获得更大的网络犯罪收益。

一旦意识到较小的市场并不能真正防范网络犯罪，了解您的企业如何成为被攻击目标的定位方式就很重要了。FBI 2023年3月10日发布的年度互联网犯罪报告中强调，每个人至少应该了解其中一个威胁：社交工程欺诈。

什么是社交工程欺诈?

传统的“黑客”依靠软件或硬件中的漏洞来获得对网络和计算机系统的未经授权的访问，而社交工程欺诈则依赖于人和情感。

根据网络安全和基础设施安全局的说法，社交工程攻击是指利用“人际互动（社交技能）来获取或破坏有关组织，或其计算机系统的信息”。

这种“人际互动”包括短信、电子邮件和语音等形式，甚至能够通过披露敏感信息欺骗谨慎的员工——尤其是当与恐惧和紧迫感等强烈情绪结合在一起时。

社交工程：10 种欺诈类型

当犯罪分子试图利用技术、信任和情感来对付您和您的团队时，熟悉他们的技术可以帮助您避免成为受害者。这种不断发展的欺诈类型的流行技术包括：

诱饵Baiting：诱饵攻击通过提供快速或轻松地访问商品的方式诱使受害者重复使用密码，或者诱使他们插入USB闪存驱动器来安装恶意软件。

商业电子邮件入侵(BEC)：在成本最高且难以检测的社交工程攻击中，BEC冒充高管来指挥下属进行欺诈性资金转移。

转移盗窃Diversion Theft：这是一种适应现代使用的古老策略，转移盗窃攻击的受害者向欺骗的位置或人员发送/获取敏感信息。

蜜罐Honeytrap：蜜罐通常带有浪漫的色彩，使用伪造的在线个人资料来欺骗受害者，使其向他认为是真实的人透露信息。

网络钓鱼Phishing：这些攻击使用来自看似值得信赖的来源的电子邮件或伪造网站，涉及广泛感兴趣的主题，以从大量人群中获取个人信息。

冒名电话Pretexting：冒充权威或值得信赖的来源，要求提供个人信息，这些信息可用于直接获得未经授权的访问，或进一步冒充其初始受害者对预期目标进行后续攻击。

交换条件Quid Pro Quo：交换条件攻击者通常冒充提供有价值的服务（例如提高网络速度或更新软件）的虚假报价，要求提供登录凭据作为先决条件。

网络钓鱼简讯Smishing：短信诈骗的设置和执行简单且成本低廉，它使用以短信形式发送的恶意链接来引诱受害者访问欺诈网站以安装恶意软件。

尾随Tailgating：是一种面对面的利用，它会用看似微不足道的礼貌（例如“我忘记了我的笔记本电脑，可以借用你的吗？”）作为访问其他受限区域和资源的一种手段。

捕鲸Whaling：这类攻击是专门的网络钓鱼攻击，针对强大的利益相关者（例如首席执行官），使用高度发达的个人信息而不是一般的大众信息。

所有这些攻击的一个共同特点是利用情感（例如，帮助他人的愿望或担心为代价高昂的错误负责）作为鼓励受害者授予攻击者访问权限的手段。

面对社交工程欺诈我该怎么办?

与往常一样，鼓励员工使用最佳实践，例如创建强密码并尽可能使用VPN，以帮助保护您的业务数据。确保您的安全策略和系统保持最新的同时，您可以采取一些重要的非技术步骤来促进网络安全：

了解威胁环境：全年花时间与联邦调查局或网络安全和基础设施安全局等权威机构保持联系。在攻击发生之前了解它，可以起到很大的预防作用。

与团队沟通：确保您的团队了解这些威胁，以及如何消除它们。每季度更新一次最新的诈骗和威胁手段，让每个人都了解情况。鼓励您的团队提问和验证，而不是因恐惧或紧迫而采取行动。通过理性和勤勉，大多数网络犯罪都是可以轻松预防的。

获得网络保险：查看并更新您的商业保险单，以确保适当的承保范围。企业主发现他们要么没有为网络犯罪投保，要么保险不足，因为许多保险公司的网络保险政策不涵盖社交工程索赔。

然而，有的保险公司例如ERIE，提供网络保险，可能涵盖因社交工程引起的索赔，解决了保单持有人的员工无意中向攻击者授予访问权限的各种网络犯罪后果，包括数据泄露、误导性付款，计算机欺诈和攻击、网络勒索，电信欺诈，恶意软件，隐私事件责任、网络安全责任和电子媒体责任的第三方责任险等。这种网络犯罪保护不仅仅解决攻击本身带来的直接影响，涵盖的索赔还包括对取证合规性、恢复等下游后果的保护。

欢迎扫描上方的二维码，了解更多保险信息。

保持最新状态，保持安全

网络安全是一个不断发展的问题，及时了解最新的威胁是避免这些威胁的一种方法。但即使您采取预防措施，网络欺诈仍然可能发生。这就是为什么确保通过正确的保险来保护您的业务如此重要。

信息出处：https://www.erieinsurance.com/blog/social-engineering-fraud?link=mainbutton&utm_source=Businesssensenews&utm_medium=email&utm_campaign=BusinessSense_September_2023&utm_content=20230927&bt_ee=4l2vQCwQ6tnf8aWODw0N9km8wmABNtIsXzE%2BeNW9cZc%3D&bt_ts=1695824023286&AgencyFromUrl=ZZ1111