公告

公元 2019 年 5 月 23 日

反制外部诈骗-网络钓鱼

会员们应该有注意到 "网络钓鱼"的诈骗手法，亦即欺诈者假装真实方以非手段法拦截资金 (打算支付给真实方的资金) 和/或获取敏感信息。 简单地说，欺诈者冒充一方当事人加入正常的往来通讯对话中。例如，可能真正的第三方电子邮件地址为 XYZ@cargo.com，但欺诈者设法使用 XYZ@carg0.com 电子邮件地址来参与对话。如果其他当事方在操作电子邮件时使用 "全部回复" 这个功能，欺诈者就会被添加到今后所有的往来对话中，并可以监看事态发展，包括何时以及要向谁支付款项。

这种性质的欺诈行为可能持续数周或数月，在预定付款或敏感信息即将被揭露之前，不会有立即明显的迹象表明讯息被人截取。

截取电子邮件

最难以被发觉的网络钓鱼行为发生在大量收件人被放置于电子邮件通信的副本中，以及各种不定期(一次性) 付款的情况下。副本中的收件人越多，电子邮件被截取并置入属于欺诈者之新的，但类似的电子邮件地址的风险就越大。

许多会员维持着高水平的网络安全标准，并保护自己免受直接网络攻击。然而，由于航运业的国际性质和适用的网络安全标准各不相同，欺诈者通常会攻击系统最不安全的当事方，以获取通信对话信息。

以电子邮件安排付款

一旦欺诈者能够截取往来讯息，他们可能会在最后一刻替换银行账户细节，使用正确的账户名称，但使用不同的账号和银行代码。银行通常不会检查接受付款的账户其持有人姓名。相反地，银行通常只是检查账号和银行代码 (IBAN)以完成付款。因此，欺诈者可以不当地使用原应接收付款的合法受款人名称，但使款项支付给诈欺者自己开立的银行账户和银行代码 (IBAN)。安排付款的一方会以为其将款项支付给正确的人，直到为时已晚。

避免诈欺之风险

协会曾经遇过各种试图网络钓鱼的非法诈骗情况，因此我们启动了一些程序以侦测并应对这些挑战，这些程序包括:

1. 确保我们的电子邮件系统尽可能地安全，包括使用高强度密码和反制网络钓鱼软件。

2. 限制参与通信对话中当事方之数量。鉴于数据保护立法 (例如欧盟的 GDPR 法规) 不断增加，这一良好做法有助于最大限度地减少没有真正参与通信的当事方不必要地看到敏感通信内容。在通讯讨论付款或银行帐户变更的细节时，这一点尤其重要。

3. 在提供付款或银行详细信息时，请避免使用 "全部回复"这个功能，而应考虑手动输入电子邮件地址或检查收件者网站或公司信纸上的电子邮件地址。验证电子邮件地址可以减少欺诈者注意到何时会有付款的情况。

4. 当第三方将其银行帐户数据之变更通知我方或首次提供新的帐户信息时，应透过其他联系方式进行交叉查验，以验证新的银行帐户信息(应再次使用以前曾经验证过的联系人信息来联系确认，而非使用通知更改付款数据时所提供的联系方式)。

5. 提高对网络钓鱼风险的认识，并鼓励员工定期检查发送或接收电子邮件时使用的电子邮件地址，且在收到对方关于更改银行帐户资料之请求时应特别有所警觉，尤其是需要紧急安排付款的情况时。

- 完 -

(译注: 英文原文若与中文翻译有出入，或用语未正确翻译或有疏忽漏译，皆以英文原文为准)