西元 2019 年 5 月 23 日

反制外部詐騙-網路釣魚

會員們應該有注意到 "網路釣魚"的詐騙手法，亦即欺詐者假裝真實方以非法手段攔截資金 (打算支付給真實方的資金) 和/或獲取敏感資訊。 簡單地說，欺詐者冒充一方當事人加入正常的往來通訊對話中。例如，可能真正的第三方電子郵件地址為 XYZ@cargo.com，但欺詐者設法使用 XYZ@carg0.com 電子郵件地址來參與對話。如果其他當事方在操作電子郵件時使用 "全部回覆" 這個功能，欺詐者就會被添加到今後所有的往來對話中，並可以監看事態發展，包括何時以及要向誰支付款項。

這種性質的欺詐行為可能持續數周或數月，在預定付款或敏感資訊即將被揭露之前，不會有立即明顯的跡象表明訊息被人截取。

截取電子郵件

最難以被發覺的網路釣魚行為發生在大量收件人被放置於電子郵件通信的副本中，以及各種不定期(一次性) 付款的情況下。副本中的收件人越多，電子郵件被截取並置入屬於欺詐者之新的但類似的電子郵件地址的風險就越大。

許多會員維持著高水準的網路安全標準，並保護自己免受直接網路攻擊。然而，由於航運業的國際性質和適用的網路安全標準各不相同，欺詐者通常會攻擊系統最不安全的當事方，以獲取通信對話資訊。

以電子郵件安排付款

一旦欺詐者能夠截取往來訊息，他們可能會在最後一刻替換銀行帳戶細節，使用正確的帳戶名稱，但使用不同的帳號和銀行代碼。銀行通常不會檢查接受付款的帳戶其持有人姓名。相反地，銀行通常只是檢查帳號和銀行代碼 (IBAN)以完成付款。因此，欺詐者可以不當地使用原應接收付款的合法受款人名稱，但使款項支付給詐欺者自己開立的銀行帳戶和銀行代碼 (IBAN)。安排付款的一方會以為其將款項支付給正確的人，直到為時已晚。

避免詐欺之風險

協會曾經遇過各種試圖網路釣魚的非法詐騙情況，因此我們啟動了一些程序以偵測並應對這些挑戰，這些程序包括:

1. 確保我們的電子郵件系統盡可能地安全，包括使用高強度密碼和反制網路釣魚軟體。

2. 限制參與通信對話中當事方之數量。鑒於資料保護立法 (例如歐盟的 GDPR 法規) 不斷增加，這一良好做法有助於最大限度地減少沒有真正參與通信的當事方不必要地看到敏感通信內容。在通訊討論付款或銀行帳戶變更的細節時，這一點尤其重要。

3. 在提供付款或銀行詳細資訊時，請避免使用 "全部回覆"這個功能，而應考慮手動輸入電子郵件地址或檢查收件者網站或公司信紙上的電子郵件地址。驗證電子郵件地址可以減少欺詐者注意到何時會有付款的情況。

4. 當第三方將其銀行帳戶資料之變更通知我方或首次提供新的帳戶資訊時，應透過其他聯繫方式進行交叉查驗，以驗證新的銀行帳戶資訊(應再次使用以前曾經驗證過的連絡人資訊來聯繫確認，而非使用通知更改付款資料時所提供的聯繫方式)。

5. 提高對網路釣魚風險的認識，並鼓勵員工定期檢查發送或接收電子郵件時使用的電子郵件地址，且在收到對方關於更改銀行帳戶資料之請求時應特別有所警覺，尤其是需要緊急安排付款的情況時。

- 完 -

(譯註: 英文原文若與中文翻譯有出入，或用語未正確翻譯或有疏忽漏譯，皆以英文原文為準)