詐欺 —— 入侵商業電子郵件

您知道要注意的危險信號嗎?

如果您在國際供應鏈行業中工作，那就有可能在正常的業務過程中，無意中接觸到多種類型的支付詐騙。這些詐騙方法往往都很複雜，涉及國際上的多方合謀。 其詐騙收益通常用於其他犯罪活動，如毒品走私、人口販賣、現代奴隸制和恐怖主義。

在當今快節奏的數位化環境中，商業交易和溝通幾乎都是透過網路進行，詐欺風險也隨之增加，使得盡職調查比以往任何時候都更為重要。本通訊將帶您瞭解全球供應鏈中最常見的支付詐欺方法，以及您可以採取的預防措施，進而減輕您的風險。

有哪些風險?

在我們的行業中，哪些類型的詐騙是最常見的?

支付欺詐

通常情況下，有一個騙子偽裝成為一個您定期支付款項的企業，會指示您將款項支付到另一個帳戶。欺詐人會監視電子郵件系統，從而等待一個合適的付款請求。他們會複製郵件的風格和語言，以確保不會被發現。通常他們所使用的電子郵寄地址與您經常發送的位址幾乎是相同的——有時甚至是完全吻合的。

CEO欺詐

CEO欺詐是一種常見的支付詐騙，即有一封似乎是來自內部郵件的指令，聲稱是公司高級管理人員發送的，要求您緊急匯一筆款項給一個新客戶或與現有客戶類似的一個新開設的帳戶。

採購欺詐

在全球供應鏈中，企業普遍依賴于分包商提供物流服務；然而，這可能會讓您暴露于詐騙者假冒分包商開具虛假發票的風險中。

詐騙者會潛入電腦系統，監控電子郵件，以收集詐騙所需的資訊。通常，偽造的發票很難與特定的委託保持一致，或者它可能是先前採購訂單的副本，但銀行資訊不同。

在尚未付款而詐騙份子想盡快迫使交易通過，可能會使用一些策略，例如在信用評級、商業地位上給予負評，並威脅採取法律行動，。

為避免成為欺詐活動的受害人，當您在工作時收到此類電郵，請考慮以下指引:

TT CLUB
IS MANAGED
BY **THOMAS**
MILLER

更多資訊

請聯繫我們的郵箱 **riskmanagement@ttclub.com**
或方位我們的網站 **ttclub.com**