商业电邮诈骗

商业电邮诈骗

伪冒电邮是骗徒常用的诈骗手法之一。

当付款到期时，骗徒可能发送一封看似由供应商发出的电邮，内容模仿真实讯息的格式与语气。他们会声称您的付款银行资料已更新，并提供新的账户资料，要求您按指示付款。

这类电邮往往难以辨识：

- 骗徒常会使用供应商的真实电邮地址，或伪装成极为相似的地址。
- 他们会制作看似真确的发票。
- 供应商员工的电邮签名亦可能毫无异样。
- 讯息内容往往带有急切语气，例如声称与敏感交易有关，需即时汇款。
- 骗徒可能已掌握整段电邮往来纪录，并能以相似语气及措辞回覆。
- 最重要的是——所要求的付款往往确实到期。
- **唯一的分别可能只是银行账户资料已被更改。**

电邮入侵如何发生？

电邮账户盗用

- 骗徒使用骇客技术或已窃取的账户资料，入侵企业的电邮账户。
- 电邮账户详细资讯可能是因网路钓鱼或资料外泄，而被骗徒获取。
- 不法份子可能会搜集有关使用者的联络人资料、邮件撰写风格和个人资料，使他们的所杜撰的讯息看起来更可信。

伪冒电邮

- 不法份子开立一个与真实电邮地址非常相似的账户。
- 或者他们可能利用伪冒的电邮格式和标题，企图令收件人不容易察觉，并将其当作为真实的邮件来回覆

冒充高层主管诈骗

不法份子假冒公司的高层人员

- 他们通常向财务部门发送电邮，要求紧急汇出一笔大额款项，原因可能是用于收购项目或其他重要交易。
- 被冒充的高层主管往往正值休假或不在办公室，令相关细节难以即时核实。
- 骗徒可能透过网络钓鱼攻击或资料外泄入侵电邮账户，并从公司网站或社交媒体收集资讯，以增加讯息的可信度。