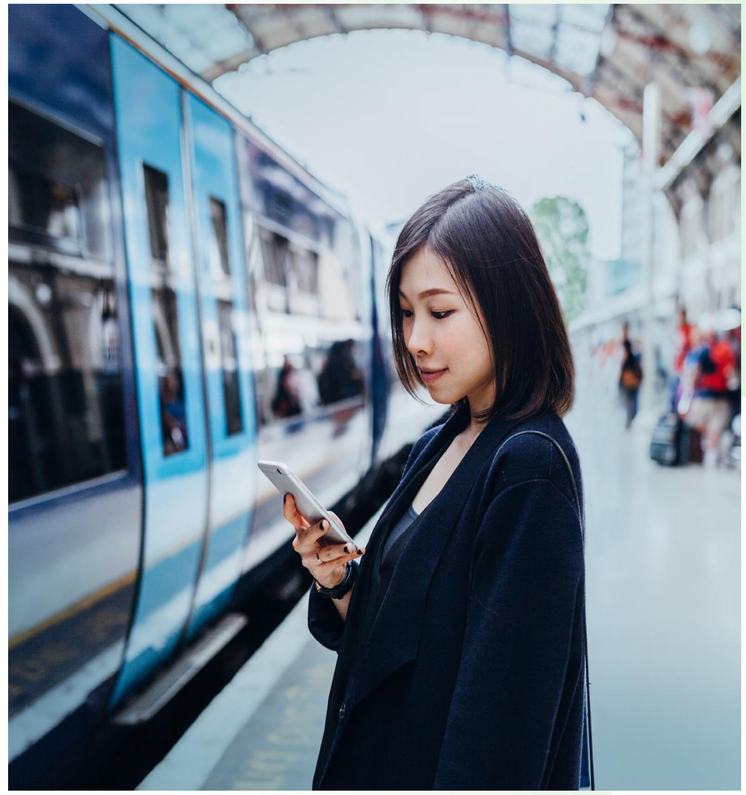
如何减少付款诈骗风险

减少付款诈骗风险

每间企业均可采取一系列简单且成本不高的措施，以减少付款诈骗及骗局的风险。防范工作人人有责。

- 在您的业务中可能存在弱点的部分培养警觉意识
- 教育员工如何识别和避免诈骗，并确保他们了解公司的安全政策和程序。
- 对任何不寻常或与业务背景不符的付款要求，应主动提出查询。
- 最重要的是，任何新增的受款人或银行账户资料，务必透过已预先建立的可靠渠道（例如已知联络人及电话号码）核实。
- 接下来的数页投影片将提供更详尽的指引，为负责付款的同事提供支援。



检查电邮地址

骗徒会冒充可信人士。

- 即使电邮署名为您熟悉的人士（如您认识或经常联络的人士），亦应核对电邮地址是否正确。
- 如发送人属公司同事，其电邮地址应可在公司通讯录中查核（如有提供）。
- 请特别留意网域名称的拼写是否正确。骗徒常会建立与真实网域极为相似的伪冒地址，只改动一两个字母，企图混淆收件人，例如 J@rnbusiness.com 与 J@mbusiness.com 。
- 显示名称可能隐藏真实的发件人电邮地址，切勿只凭表面判断。

仔细检查电邮

「紧急要求」是常见的警号。

- 如电邮涉及付款事宜，且语气紧急或声称无法回电，应视为可疑讯息。
- 部分网络钓鱼电邮语句粗疏，即使拼字正确，语法亦可能错误。对外来电邮务必保持高度警觉，尤其是含有连结或附件者。请注意：生成式人工智能令骗徒更容易制作自然语气、内容逼真的恶意电邮。
- 如您并未预期收到该讯息，或不认识发件人，切勿点击连结或开启附件。

新受款人或变更账户资料均需核实

请务必透过已知联络方式与指示方核实其要求。

- 在可行的情况下，应致电您熟悉的联络人进行确认。例如：如变更付款资料要求来自公司内部人员，请直接致电该同事确认；如变更要求来自供应商，请致电您经常联络的负责人，并同时核对银行代码及账户号码。
- 切勿直接回覆该电邮或使用电邮内所提供的联络方式。
- 一般情况下，网络不法分子在获得登入账户权限后，会向账户联络清单上的相关人士发送钓鱼邮件。这代表着即使电邮的内容相当可疑，您仍可能会因为电邮地址正确无误，而认为真的是由该寄件人发出。此时，您应致电该寄件人，既可以确认电邮中的要求，亦可提醒他们的电邮账户或已遭入侵。

减低付款诈骗风险

任何类型的企业均可能面对诈骗风险，手法亦多不胜数。

制定及落实有关汇款的保安机制

确保所有付款均经妥善核实，是防止诈骗最关键的一步。建立既定的程序，防止汇款团队在未经核实的情况下授权新增或更改的付款指示。按照所订立的保安机制，就可确保汇款团队不会仅根据，看起来真实的付款指示，未经验证的电邮或电话指示转移资金。此外，也应鼓励员工直接联络收款人以确认新的或变更的付款要求。

提高员工警惕性

企业应为员工提供充足的培训，教导员工防诈骗是公司任何一员的责任，并建立一套能让员工向管理层安心反映疑虑的企业文化。

审慎管理您的数码足迹

在社交媒体平台上过度分享个人资讯，可能令骗徒掌握您、您的朋友、家人及联络人的资料，并用作冒充身份。减少公开个人资讯，有助降低成为攻击目标的风险。

鼓励员工三思而后点击

点击可信任的网站上的连结虽然无妨，但点击未经验证电邮和即时讯息中的连结，则应可免则免。将鼠标悬停在连结上，您便可看到隐藏的网址并验证其真实性。在点击任何电邮内的连结或下载任何附件之前，请再三查证，尤其应注意是否出现拼写和文法错误。

加强您的密码可靠性

请考虑使用密码管理器或密码短语。密码短语通常比传统密码更长，但更容易记住且难以破解。鼓励员工随机选择三个单词，并选择字母、数字和符号组合，以加强密码的可靠性。

在遇上诈骗/网路攻击时应采取的措施

如果您或您的公司不幸成为诈骗/网路攻击的受害者，请迅速采取应对措施。及时举报已发现或疑似的事件有助于保障公司免受进一步的攻击，减低损失。请尽快与您的银行或相关的的财务机构联络，以确保及时得到所需的支援。.