检查清单：处理付款–第 1 / 2 部分

在最容易受诈骗威胁的业务范畴，应时刻保持警觉及采取合适的行动，请参考下列建议，有助相关的人员以更严谨的方法处理付款指示，并培养对诈骗有警觉性的企业文化。

- ❑ **想一想：该要求是否不寻常或与业务背景不符？是否合乎逻辑？**任何涉及汇款或账户资料的电邮，如语气紧急或声称无法回电，均应视为可疑。如您并未预期收到该讯息，或不认识发件人，**切勿点击任何连结或开启附件。**
- ❑ **请核实电邮地址是否属真实及可信。**即使电邮署名为您熟悉的人士（如您经常联络的人士），亦**应核对电邮地址是否正确。**骗徒会冒充可信人士。如属公司同事，其电邮地址应可在公司通讯录中查核（如有提供）。

  另外，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。
- ❑ **即使汇款指示来自高级管理层，也应保持警觉，提出质疑。**骗徒深知员工更倾向听从高层指示，因此常会冒充高级主管或业务伙伴发出付款要求。切勿单凭电邮内容信任付款指示，即使发件人身份看似可信。骗徒亦可能透过常用的即时通讯平台进行诈骗。

请注意，骗徒有可能已入侵并取得您正在通讯的电邮账户的存取权限

检查清单：处理付款–第 2 / 2 部分

核实新增或更改的付款资料，有助减低付款诈骗的风险。除了回拨电话加以确认，还有多项重要措施可进一步减低风险。

- **核实新收款人或账户的资料变更**
  在可行的情况下，请使用可靠的联络方式向对方查证，并请尝试与您相识的人确认。例如，如果变更请求来自公司内部人员，请直接致电该人员以作确认。如果来自供应商，请致电与您经常联络的人员以作确认。请勿回覆电邮或使用电邮中的联络方式。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。
- 切勿直接回覆该电邮或使用电邮内所提供的联络方式。如骗徒已入侵他人账户，他们极有可能更改联络资料，令您最终与骗徒通话。
- 请主动致电付款指示方确认，切勿依赖对方来电。骗徒深知回拨核实是常见程序，可能会先行联络您，以避开此步骤

请注意，骗徒有可能已入侵并取得您正在通讯的电邮账户的存取权限