# 商业电子邮件攻击欺诈

## 供应商安全警报。

### MSD 公司非常重视欺诈和信息保护。

请注意，随着我们对虚拟通信的日益依赖，商业电子邮件攻击 (BEC) 的发生率呈上升态势。BEC 会使用电子邮件和其他电子通信方式冒充企业的高管、员工或其他职权人员，然后代表企业提出欺诈性的付款请求，或获取员工薪资或 W2 (仅限美国) 信息。

### 须知事项

MSD 公司致力于保护您的企业和银行信息。我们训练有素的员工遵从我们全球隐私办公室的指示、我们的信息技术流程和指南，以及当地和地区的法规，对数据的收集、验证和获取采取严格的流程和控制措施，不仅设有多个检查点，还会对我们的程序和做法进行定期审核。

为了更好地保护您的企业：

- 请使用双重渠道，或双重身份验证来独立验证对帐户信息的更改请求。
- 确保电子邮件中的 URL 与发件人自称的所属企业有关联。
- 对实际域名存在拼写错误的超链接保持警觉。
- 验证发送邮件的电子邮件地址，确认其与发件人相符，特别是在使用移动设备或手持设备时。
- 创建入侵检测系统过滤器，以标记扩展名与公司电子邮件相似的电子邮件。例如，如果 ceo@abc_company.com 是合法电子邮件，则发自 ceo@abc-company.com 的邮件会被标记为欺诈电子邮件。
- 定期监控财务账目是否存在异常情况，如存款丢失。
- 及时安装所有软件补丁，并将所有系统更新到最新状态。
- 对员工计算机进行设置，确保能看到完整的电子邮件扩展名。
- 保存您当地解决中心的联系信息，如果您觉得自己是 BEC 的受害者，并且该情况与默克公司或 MSD 有关，请向该中心发送警报；另外，您也可以联系当地的执法部门。

默克公司在美国和加拿大以外被简称为 MSD。