汇丰诈骗防范意识

保护你的企业免受诈骗和网络犯罪的威胁

汇丰
HSBC

保护你的企业免受诈骗威胁

近年来，诈骗已成为企业最常面临的威胁之一。

稍有不慎，便可能招致重大的财务损失。不论企业规模大小，都会随时面临同等的威胁，因此，本指南旨在帮助你和你的员工及早辨识诈骗危机，作出有效的预防措施。如你不幸成为受害者时，也可采取正确的应对措施。

高达430亿美元

2016年6月至2021年12月全球商业电子邮件诈骗所造成的经济损失

数据源：FBI互联网犯罪投诉中心

本指南将帮助你认识可能会威胁你业务的常见诈骗类型，并提供一些实用的防诈骗方法。防御诈骗的相关教育可使企业及业务获得更全面的保障，本指南提供了一系列的反诈方法和自检清单，可供管理及支付团队进行参考。

可能威胁你业务的诈骗类型

汇丰
HSBC

在付款时遭受诈骗的风险特别高

- **授权支付** (APP) 诈骗是指骗徒冒充真正的收款人，欺骗企业将资金汇到骗徒手中。
- 网络钓鱼是APP 诈骗的常见方法，骗徒会试图欺骗用户点击一个虚假链接，该链接实则下载恶意软件，或将用户引导至虚假网站。
- 网络钓鱼也可能试图伪装成你信任的联络人或者你的银行，以获取敏感信息，如用户名称、密码和账号详细信息。

商业电子邮件诈骗

骗徒常用伪冒的电子邮件进行诈骗。

临近付款期，骗徒会发送一封看起来像供货商发送的真实电子邮件，告知你收款银行的详细信息已更改，并将更新后的信息提供给你要求你付款。
此类诈骗往往难以识别，因为：

- 骗徒通常使用供应商所常用的电子邮箱地址，或看起来与该电子邮箱地址非常相似的伪冒电子邮箱地址。
- 骗徒所签发的收据仿真度极高。
- 伪冒的供应商职员电子邮件签名或沟通风格，均可能与真实的没有明显差异。
- 在某些情况下，骗徒可能已经获得了登入邮箱的权限，因此该诈骗邮件是来自一个真实的电子邮箱地址。骗徒将能够存取邮件链接并模仿相似的话术和文字进行交流。
- 骗徒所要求的款项，往往是即将到达付款期限的款项。
- **通常来看，此类电子邮件跟真正供应商的电子邮件的唯一区别，是收款银行的详细信息发生了变化。**

电子邮件诈骗的成因

电子邮件账号被入侵

- 骗徒使用黑客技术或已窃取的账号信息，入侵企业的电子邮件账号。
- 电子邮件账号的详细信息可能会因网络钓鱼或数据外泄，而被骗徒获取。
- 不法份子可能会搜集有关用户的联络人、邮件撰写风格和个人资料，使他们的伪造的内容看起来更可信。

伪造电子邮件

- 不法份子开立一个与真实电子邮箱地址非常相似的账号。
- 或者他们可能利用伪造的电子邮件格式和标题，使收件人混淆，并将其当作真实的邮件来回复。

冒充高层主管诈骗

不法份子假冒公司的高层人员

- 他们将发送电子邮件给会计部门，要求紧急支付一笔大额款项，原因可能是用于收购项目或其他重要交易。
- 他们通常会选择高层人员不在公司时进行诈骗，让对方难以查证核实。
- 再次强调，电子邮件账号可能经由网络钓鱼或数据泄漏而被入侵，而入侵所需的相关信息往往是通过公司网站或社交媒体的渠道收集而来。

其他常见的诈骗攻击方式

语音钓鱼和电话诈骗

电话诈骗，或称语音钓鱼，是指诈骗者假冒成你的银行或其他可信任的机构来进行电话诈骗。他们甚至可能让来电号码显示成你认识且信任的号码，此被称为改号欺诈。

诈骗者的话术听起来非常真实可信，甚至可能已经掌握了一些关于你的个人信息，如账号号码或地址。如果你觉得有任何不妥，或察觉异常，请不要犹疑，立即挂断电话。你可以反过来致电你知道的机构电话号码，例如你银行卡背面的电话号码，以核实来电的真伪。

但请留意，骗徒可能还继续保持着通话线路的连通，甚至伪造拨号的音效，让你误以为你真。因此，请使用另一部手机，或相隔至少30秒后再致电。
常见的例子包括：

- “你的银行”通知你的账号出现风险，需要将你的资金转移到另一个账号，以确保安全。
- “你的银行”需要你的协助来调查诈欺事件。
- 你的网络服务商或通信运营商致电给你，替你解决你从没有报告过的问题。

银行可以根据你的要求转账，但绝不会因此索取你的密码、PIN码、任何一次性密码或安全代码。

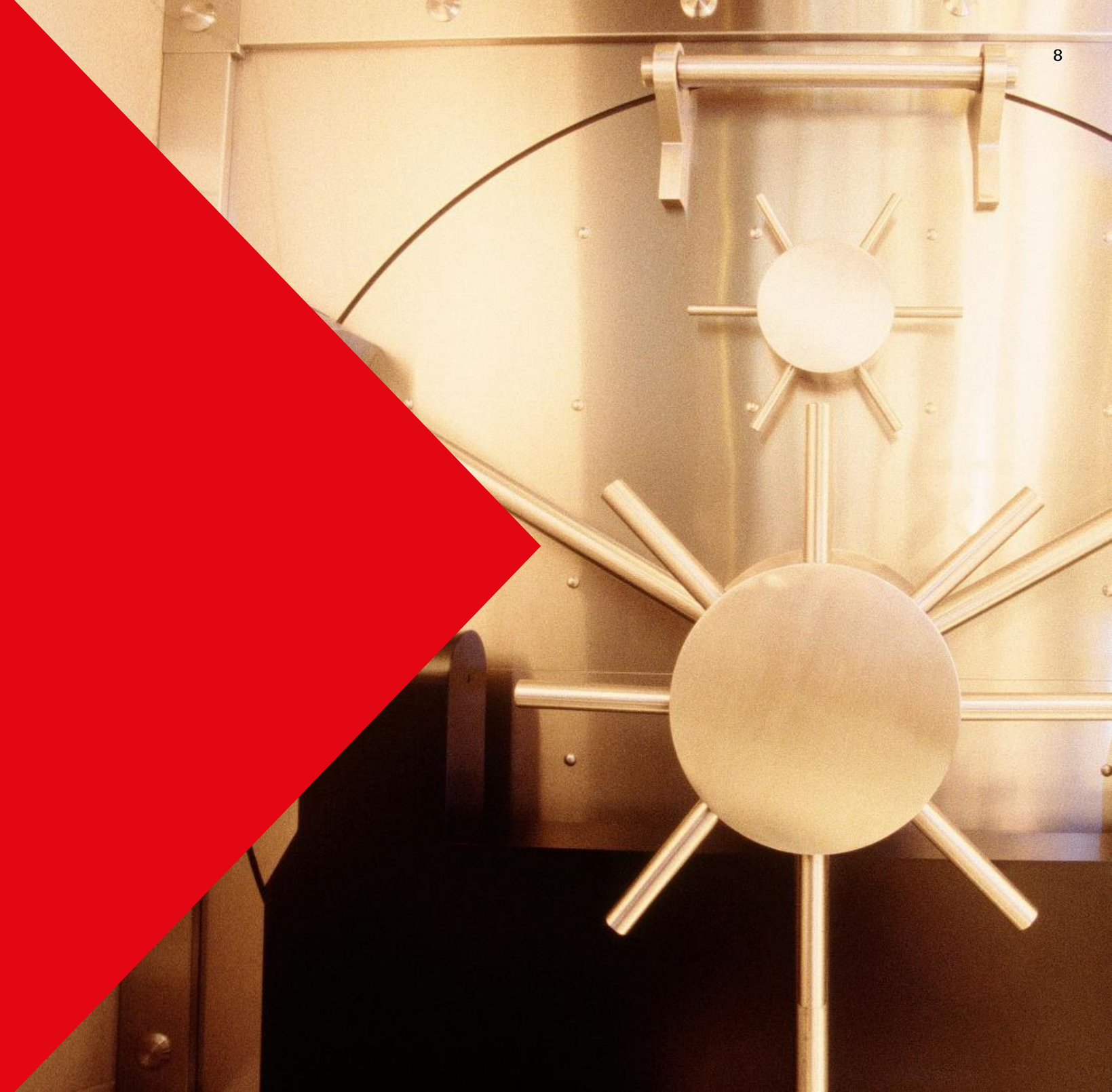
入侵账号欺诈

骗徒可能以伪冒的电话号码致电给你，例如显示为汇丰电话银行或其所伪冒公司的电话号码。骗徒往往对公司的运作相当熟悉，会引导你操作你所预期的流程，例如验证程序，以博取你的信任。
接着，他们将以各种方法来骗取你的安全信息，例如用户名称、密码、安全代码。骗徒随后可以使用这些信息，成功入侵你的账号，转走资金。

请谨记：

- 汇丰银行不会要求你提供卡片PIN码、密码或安全代码。
- 不要向任何人透露安全代码。
- 汇丰银行绝不会要求你将资金转移到任何安全账号。

防止诈骗



汇丰
HSBC

降低诈骗风险

每家企业都可以采取一些措施来降低诈骗风险。这些措施既不复杂，也无需花费高额成本。

- 评估你的业务，在最易受诈骗威胁的部份提高警惕。
- 教育员工如何辨识和避免诈骗，并确保他们了解公司的安全政策和措施。
- 最重要的是，任何新的收款人或账号的详细数据都必须经过核实。
- 对任何异常或不合理的请求，必须作出进一步的查询。
- 接下来的内容，将为负责付款的人员，提供更详细的指引。

确认电子邮箱地址

骗徒会伪冒成信赖的人士。

- 如果邮件发件人的名字相当熟悉（你认识或经常通信来往的人），请**确认电子邮箱地址是否相符**。
- 如果发送人是同事，其电子邮箱地址应列在公司的电子邮件目录上（如有）。
- 确认域名的拼写是否正确。诈骗者经常会创建与真实域名非常相似的假域名，通过更改一个或两个字母，使收件人混淆或不易察觉。例如：J@rnbusiness.com 及 J@mbusiness.com。
- 请注意，电子邮件显示的名称可能与实际发件人的电子邮箱地址不符。

仔细审查电子邮件

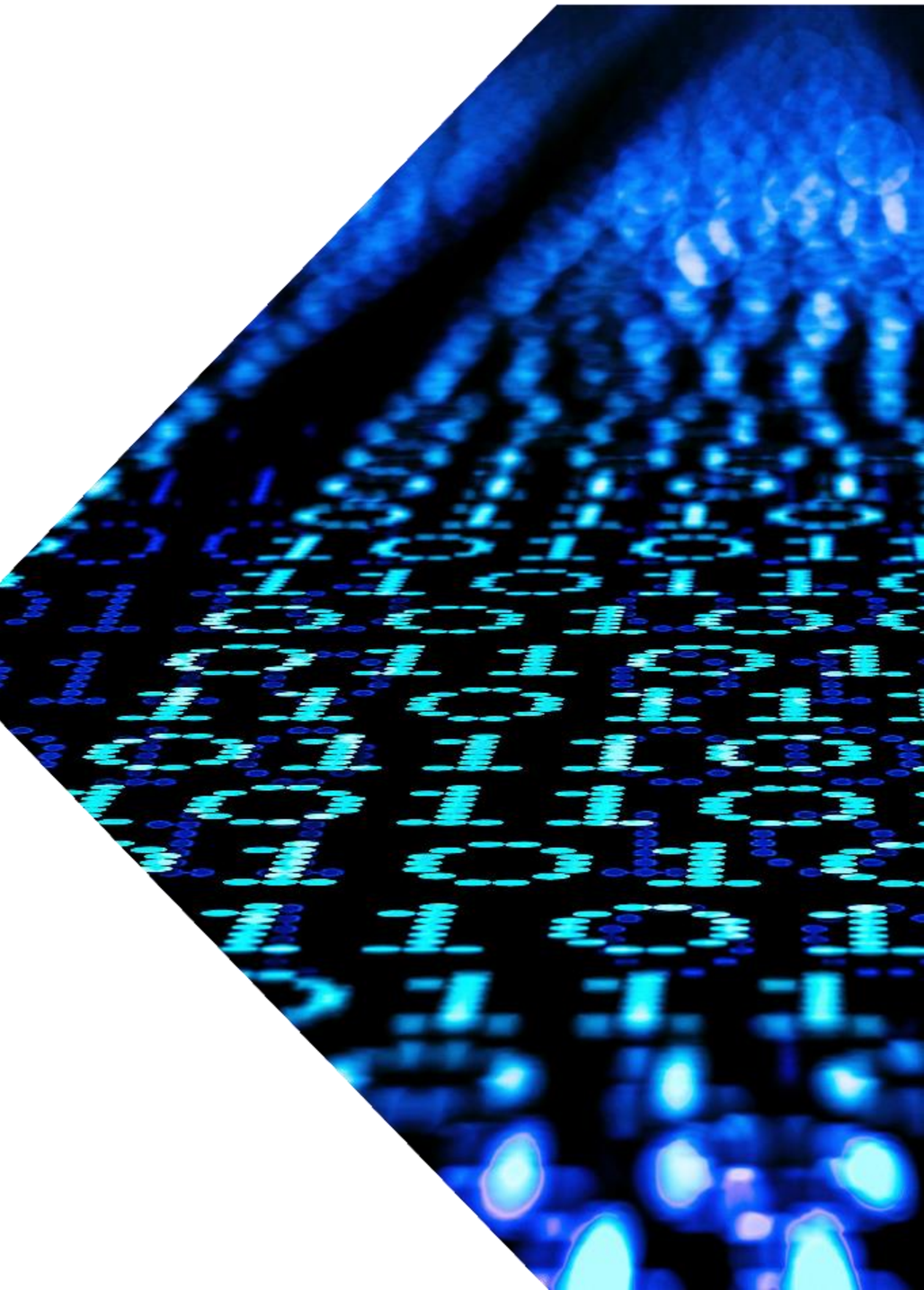
声称紧急情况更需要警惕

- 如果任何与付款事宜相关的电子邮件，使用了紧急的语气，或以没有回电选项为借口，则应视为可疑电子邮件。
- 一些钓鱼邮件写得相当糟糕，即使拼写正确，也可能出现文法错误。对从外部发送过来的电子邮件应加倍警惕，特别是那些包含链接或附件的电子邮件。请注意，生成式人工智能使骗徒更容易杜撰出更真实可信的恶意电子邮件。
- 如果你收到非正常的电子邮件，且/或不认识发件人，**请勿点击电子邮件内的链接或打开附件**。

核实新收款人或账号的数据变更

请使用可靠的联络方式向对方查证。

- 在可行的情况下，请尝试与你认识的人联络。例如，如果公司内部人员要求资料变更，请直接致电该人员进行确认。如果变更要求来自供应商，请致电与你经常联络的人员进行确认。
- **请勿回复电子邮件或使用电子邮件中的联络方式。**
- 一般情况下，网络不法分子在获得登入账号的权限后，会向账号联络清单上的人士发送钓鱼邮件。这代表着即使电子邮件的内容相当可疑，你仍可能会因为电子邮箱地址正确无误，而认为真的是由该发件人发出。此时，你应致电该发件人，确认电子邮件中的要求，并提醒他们电子邮件账号或已遭受入侵。



防止诈骗

任何类型的企业均有机会遭受不同形式的诈骗。幸而，你可以采取一些措施来让你的企业免受诈骗和网络犯罪的威胁。以下是一些可以帮助你降低企业内部诈骗风险的实用建议和自检清单。

建议

制定及落实有关企业付款的保安机制

防范诈骗的关键在于确保所有款项都经过充份的验证才支付。因此，企业应建立机制防止负责付款的团队在未经充份验证的情况下，就授权新的或被要求变更的付款。按照该建立的保安机制，就可确保负责付款的团队不会仅根据看起来真实的付款指示，未经验证的电子邮件或电话指示转移资金。此外，还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，教育员工防诈骗是公司每一位成员的责任，并建立一套能让员工安心地向管理层反映疑虑的企业文化。

鼓励员工三思而后点击

点击可信任的网站上的链接虽然无妨，但点击未经验证的电子邮件和即时消息中的链接，则应可免则免。当你可将鼠标悬停在链接上时，便可看到隐藏的网址并验证其真实性。在点击任何电子邮件内的链接或下载任何附件之前，请再三核实，尤其应注意是否出现拼写和语法错误。

加强你的密码可靠性

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/网络攻击时应采取的措施

如果你或你的公司不幸成为诈骗/网络攻击的受害者，请迅速采取应对措施。

及时举报已发现或疑似的诈骗/网络攻击事件有助于保障公司免受进一步的攻击，降低损失。

请尽快联络你的财务机构和保险公司，以确保及时获取所需的支持。

自检清单：高层管理人员

最有效抵御诈骗的方法，就是防范于未然。以下自检清单可为你提供一些实用的建议，帮助你保护企业的网络安全

- [ ] 对于全新或经过修订的付款指示，贵公司有否制定了必须作出验证的机制？员工是否知道如何取得已知联络人的信息？
- [ ] 贵公司有否制定了付款指示的保安机制？包括如何申请付款指示、由谁审核、以何种方式支付，以及在遇上疑惑时该如何验证付款指示？
- [ ] 密码的安全强度是否足够（例如：最小字符长度及使用字母、数字和符号的组合）。贵公司是否正在考虑使用密码管理器或规定使用密码短语？
- [ ] 贵公司是否有考虑应用双重验证机制及其可行性？
- [ ] 假如发生欺诈性付款时，你的员工知道如何应对和处理吗？
- [ ] 对于网络钓鱼攻击，例如电子邮箱遭到入侵等威胁，贵公司是否制定了应变计划？
- [ ] 你是否定期与提交付款指示的相关人员，讨论诈骗的潜在风险

自检清单二：处理付款要求

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，并培养对诈骗具备警觉性的企业文化。

确认电子邮箱的真伪

如果电子邮件发件人的名字相当熟悉（你认识或经常通信来往的人），请**确认电子邮箱地址是否相符且准确。**

如果发件人是同事，其电子邮箱地址应列在公司电子邮件目录上（如有）。此外，请确认域名的拼写是否正确，需要特别留意的是，诈骗者经常会创建与真实域名非常相似的假域名，通过更改一个或两个字母，使收件人混淆或不易察觉。例如：J@rnbusiness.com 及 J@mbusiness.com。最后，请仔细检查电子邮件显示的名称，可能与实际发件人的电子邮箱地址不符。

仔细审查电子邮件

任何与付款事宜相关的电子邮件，如若使用了紧急语气，或以没有回电选项为借口，则应视为可疑电子邮件。一些钓鱼邮件写得相当糟糕，即使拼写正确，也可能含有语法错误。对从外部发送过来的电子邮件应加倍警惕，特别是那些包含了链接或附件的电子邮件。请注意，生成式人工智能使得骗徒更容易杜撰更真实可信的恶意电子邮件。如果你收到非正常的电子邮件，且/或不认识发件人，**请勿点击电子邮件内的链接或打开附件。**

核实新收款人或账号的数据变更

在可行的情况下，请使用可靠的联络方式向对方查证，并请尝试与你认识的人确认。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，请致电与你经常联络的人员以作确认。请勿回复电子邮件或使用电子邮件中的联络方式。一般情况下，网络不法分子在获得登入账号权限后，会向账号的联络清单上的人士发送钓鱼邮件。这代表着即使电子邮件的内容相当可疑，你仍可能会因为电子邮箱正确无误，而认为真的是由该发件人发出。此时，你应致电该发件人，确认电子邮件中的要求，并提醒他们电子邮件账号或已遭入侵。

我们应评估所收到的请求，是否合理？有否异常的地方？

假如遭受诈骗应如何应对

汇丰
HSBC

如果你不幸成为诈骗受害人

立即采取适当措施，可把诈骗所造成的损失降到最低，同时也会提高追回资金的可能性。

- **停止与骗徒的一切联络。**
- **尽快通知所有相关人士和组织**（员工、客户和财务机构），立即联系银行，发出退款指示。因为资金转移速度非常快，一旦资金发生转移，退款程序便会更加困难。
- 向有关部门**举报诈骗活动。**
- **查看你的财务记录**，以辨识任何未经授权的交易或可疑活动。
- **保留所有与诈骗相关的证据**，包括电子邮件、收据和任何其他通讯，以便日后取证之用。
- **检讨并改善公司的保安政策和措施。**

汇丰 HSBC

向汇丰银行举报诈骗

如你怀疑有未经授权的诈骗性转账或账单支付，或怀疑企业的网络安全受到威胁，请立即致电汇丰24小时工商金融服务热线+852 2748 8288或致电你的客戶經理。

我们同时建议你通过香港警务处电子报案中心 https://www.police.gov.hk/ppp_sc/contact_us.html 举报个案。

如果你是汇丰财资网客户，请立即将相关诈骗性交易资料发送给你的客户经理，包括：

- 汇丰财资网客户编号
- 公司名称
- 汇丰财资网使用名称
- 指示参考号码

你可致电你的客户经理或者通过以下电话联系反欺诈组去确认事情的跟进

- 国际长途 + 1 778 452 2774
- 免费电话 （仅限于美国和加拿大）1 866 979 4722
- 免费电话 （仅限于英国）0800 169 9903

汇丰 HSBC

如果你遭受网络攻击，请采取以下措施：

- **关闭所有受影响设备的网络联机**，以防止恶意软件散布或未经授权的入侵。
- **更改所有受影响账号的密码**，包括电子邮件、网络和其他可能泄露了信息的账号。
- 聘用信誉良好的网络保安公司，对你的系统进行**全面检查**，以检测其他漏洞或入侵活动。
- **尽快通知所有相关人士和组织**，例如员工、客户和监管机构，并为他们提供所有相关的信息。
- **确定攻击来源**，并采取措施，防止未来再次发生遭受类似的攻击。

术语概览

诈骗和网络安全术语须知

- **防病毒软件** - 用于预防、侦测，甚至移除恶意软件的计算机程序。
- **自带设备政策**（BYOD） - 由企业实施的政策，允许员工将自己的个人电子设备用以公务用途。
- **常见漏洞与揭露**（CVE） - 列出已知安全漏洞的公开可用清单，并提供独有的ID编号、描述和参考数据以便供公众查阅。
- **加密货币** - 可像商品一样交易的端对端去中心化电子货币。
- **网络攻击** - 对计算机系统、网络、基础设施或设备的恶意攻击。
- **网络事件** - 国家网络安全中心（NCSC）定义为“违反系统安全政策以影响其完整性或可用性和/或未经授权访问或试图访问系统的行为；符合《滥用计算机法》（1990年）”。
- **暗网** - 网络的其中一部分，但无法在搜索引擎搜索出来，仅能通过特殊权限或软件访问。
- **数码足迹** - 使用网络后留下的数据踪迹，可能包括被动信息，如存储的Cookie，或者被主动发表在网络上的信息，如社交媒体帖子。
- **加密** - 使用数学算法将数据打乱的过程。这些数据可以是静态加密，例如储存在硬盘中的数据，亦可以是传输中的数据，例如透过 HTTPS 从你的网页浏览器传送到银行服务器的数据。加密了的资料并不能代表网络上的不法份子无法截取，只是已被转换为无用的和无法理解的乱码，让不法份子无机可乘。
- **防火墙** - 根据特定规则，监控网络进出流量的网络安全系统。
- **黑客** - 专门从事计算机网络攻击的人士。“黑帽黑客”进行恶意攻击，而“白帽黑客”则进行有助于网络防御的行动。
- **恶意软件** - 以达成不法或恶意目标的程序，涵盖多个方面，例如提供远程访问、加载或植入其他恶意软件、窃取银行信息、加密并拒绝存取数据，或盗用设备的运算能力。
- **安装补丁** - 安装修补程序以更新现有软件或硬件，修复已发现错误和漏洞的过程。
- **渗透测试（pen testing）** - 机构利用黑客的攻击手段来检测自身网络的安全性，通常由“红队”或专业的“白帽黑客”团队负责。

- **钓鱼** - 通常通过电子邮件欺骗收件人泄露敏感信息、点击恶意链接和/或打开恶意附件。不法份子常用钓鱼以取得设备或网络上初始入侵管道。
- **勒索软件** - 封锁或限制用户存取数据的恶意软件，并要求受害者支付赎金才能解除限制。
- **短信钓鱼** - 透过短信发送的钓鱼信息。
- **社交工程** - 操控他人心理而使其执行某种行为，通常用于骗取个人资料。
- **鱼叉式网络钓鱼** - 针对特定人士或群体所发出的钓鱼信息。
- **特洛伊木马** - 伪装成看似无害的档案或程序，让受害者以为可安心开启。特洛伊木马十分常见，通常通过钓鱼邮件传送，或者由其他称为“载体”的恶意软件传送。
- **双因素身份证（2FA）** - 一种要求用户提供两种身份识别要素的验证过程，例如已知密码和一次性密码（OTP）。一般来说，这些要素可分为：“认知要素”（密码）、“生物特征”（指纹）或“持有物件”（密匙卡）。
- **虚拟专用网（VPN）** - 允许在公共基础设施上建立安全私人的联机，最初由机构开发，以对访问内部网络资源，例如电邮服务器或共享活页夹等的员工进行身份验证。现在，越来越多的人使用消费者VPN来作为建立及选取VPN服务器的加密联机，并使用该服务器连接到其他互联网资源。
- **语音钓鱼** - 通过电话进行并大量利用社交工程的钓鱼攻击。
- **零日漏洞** - 在补丁或更新发布之前所发现到的漏洞。利用此类漏洞的恶意软件通常被称为零日漏洞攻击。

生成式人工智能（AI）和诈骗

HSBC

生成式人工智能和诈骗

骗子可能利用生成式人工智能来欺骗个人和企业，为了保护您或您的企业免受诈骗威胁，本指引将助您进一步了解不同类型的诈骗手法，以及需要注意的事项。

如何运用生成式人工智能进行诈骗？

- **网络钓鱼邮件** — 虽然网络钓鱼邮件仍是常见的诈骗方法，骗子透过人工智能，甚至可以模仿受信任者的语气和态度制作出更巧妙的诈骗**邮件**。增加了钓鱼**邮件**的辨认难度。

- **语音钓鱼**— 语音钓鱼利用生成式人工智能复制一个人的声音，甚至能像聊天机器人一样表达特定的语句。相较于其他诈骗手法，虽然语音诈骗情况并不常见，但这项技术仍然能够协助骗子成功诈骗

- **深度伪造技术** — 深度伪造利用生成式人工智能来复制一个人的外貌和声音。深度伪造视频非常真实可信，可以模仿被复制的人说出从未说过的话语。与语音钓鱼相似，深度伪造诈骗案例并不常见，但仍然需要提高警觉。

什么是人工智能?

- 人工智能（AI）是一项可以让电脑模仿人类思维执行各种工作和决策的技术。人工智能够通过分析大量数据并不断学习，从而使所作出的决策更贴近人类思维模式。

- 随着人工智能接收及分析更多数据，人工智能的决策将不断改进，并能够做出与人类相似的决策，这使得骗子更容易冒充人或企业。

如何避免受到这些威胁？

深度伪造增强了骗子诱骗受害者的能力。虽然如此，很多现行的控制措施仍然能有效地降低这些风险。下面介绍了一些关键的控制措施。

谨记常见的诈骗防范手段

- 仔细检查和验证您在短信/电子邮件/网络上看到的信息，尤其是在任何人都可以发布帖文的论坛或网站。如果您不确定信息真伪，请与你的客户经理确认。
- 留意那些要求你快速采取行动的短信/电子邮件/网络/影片——这通常是诈骗的迹象
- 留意任何需要获取您的个人信息、账户信息和财务信息的要求，汇丰员工绝不会通过电子邮件或短信要求您提供这些信息。
- 尽可能只接受来自于经批准的公司通讯渠道的付款指示。骗子通常会通过 WhatsApp 等开放通讯渠道联系受害者，因为他们无法访问经批准的公司通讯渠道。

流动保安编码

流动保安编码是具有唯一性和时效性，分发给授权人员的代码。这些代码可用于验证通讯和交易，骗子难以复制，从而增加了防御。你可参照以下方式有效使用流动保安编码：

- 切勿向未经授权的人员透露您的任何身份验证方法，包括发送到您注册的行动或安全设备的密码、一次性安全代码和一次性密码 (OTP)
- 保密传送：透过加密电子邮件等安全管道，或在必要时透过内部安全平台将这些程式码分发给授权人员。

人为监督及培训

- 人为监督：针对大额交易或异常交易的审核，制定适当的内部控制机制，可包括设置了交易限制/规则的系统控制，多人核实以执行交易，日终跟踪异常交易。对于重要的交易，建议面对面进行
- 深伪防诈意识：引导员工了解深度伪造技术的风险以及骗徒如何将其用于欺诈。培训应涵盖如何识别潜在的深伪诈骗、遵守保密协定的重要性，以及如何报告可疑活动。
- 网络钓鱼防范意识：为员工提供持续的培训，帮助你的员工识别并恰当地应对网路钓鱼攻击。网络钓鱼攻击通常是更复杂攻击的前兆。
- 模拟攻击：使用网路钓鱼模拟攻击来帮助员工识别和回应欺诈性通讯。

如何分辨深度伪造技术 - 额外指引

随着人工智能急速的发展，网络诈骗层出不穷，亦意味着将来更难以辨识真假，因此更需要提高警觉。在辨识深度伪造时需要注意以下几点。另外您也可以考虑加强控制。

1. 眼镜会产生反光，无法完美呈现光照的自然物理特性
2. 面部表情不自然或五官位置异常，或身体移动方式不自然
3. 头发或皮肤可能呈现模糊或异常移动
4. 口型无法对上。注意聆听音调和音量的变化。
5. 背景可能与聊天场景不符。可能会显示奇怪的反射或异常现象。
6. 似乎没有开灯或有奇怪的阴影。

免责声明

资料包中的某些资讯是由香港上海汇丰银行有限公司（「本行」）根据可靠但未经独立核实的资讯来源而准备。编制资料包所载的内容及资讯时，本行已严谨处理，但不对其准确性或完整性做出任何担保、陈述或保证，也不承担任何责任或义务。除特别说明外，所表达的意见仅代表本行的意见，如有更改，恕不另行通知。

免责声明中英文本如有任何歧义或不一致，概以英文本为准。