恒生銀行
HANG SENG BANK

恒生防诈骗指引

保护您的企业 免受诈骗和网络犯罪的威胁

保护您的企业免受诈骗威胁

对现今企业来说，诈骗是其中一种最常面临的威胁。

稍一不慎，诈骗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，本指引旨在助您和员工能及早辨识诈骗危机，并作出有效的预防措施。如您不幸成为受害者时，亦可采取正确的应对措施。

高达26.9亿港元

与 2022 年同季度相比，2023 年第一季香港诈骗案件增加了 65%，2023 年第二季度则增加了 42% 。 2023年上半年香港诈骗案所造成的总损失，与去年同期比较上升两成八

资料来源：香港警务处

本指引将助您进一步认识可能会威胁您业务的常见诈骗类型，并提供一些实用的防诈骗方法。如果您可在的机构中，对各成员进行相关的教育，将可让企业获得更全面保障。本指引提供了许多建议和检查清单，可供管理阶层和处理交易的支付团队参考。

可能威胁您业务的诈骗类型

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。
- 网路钓鱼是APP 诈骗的常见方法，则是骗徒试图欺骗用户点击一个连结，该连结将下载恶意软体，或将用户引导至虚假网站。
- 网路钓鱼亦可能试图伪装成您信任的联络人，例如您的银行，以获取敏感资讯，如用户名称、密码和账户详细资讯。

商业电子邮件诈骗

骗徒常用伪冒电邮进行诈骗。

当付款期到时，骗徒会发送一封看起来像供应商发送的真正电邮，通知您收款银行的详细资讯已更改，并提供已更新的资讯及要求您付款。

此类诈骗往往难以被发现，因为：

- 骗徒通常使用供应商所常用的电邮地址，或看起来与该电邮地址非常相似的伪冒电邮地址。
- 骗徒所签发的收据仿真度极高。
- 伪冒的供应商职员电邮签名或沟通风格，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，因此该诈骗邮件将来自一个真实的电邮地址。骗徒将能够存取邮件连结并以相似的语调和文字进行交流。
- 骗徒所要求的款项，往往是即将临近付款期限。
- 跟真正供应商电邮的唯一的区别，通常是更改了收款银行的详细资料。

电邮诈骗的成因

电邮账户被入侵

- 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

- 他们将发送电邮给会计部门，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。
- 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，电邮账户可能是透过网路钓鱼或资料外泄而被入侵，而入侵所需的相关资资料往往是透过公司网站或社交媒体收集得来。

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，是指诈骗者假冒成您的银行或其他可信任的机构来进行电话诈骗。以现时的人工智能技术(例如:深度伪造技术)，骗徒能从图像撷取你的容貌伪造成影片。此外，深度伪造技术还可透过声音模仿，只需撷取你五秒钟的对话，骗徒便能使用此技术模拟你的声音来创造不同的对话。因此，骗徒可以借助深度伪造影像和声音制作出根本不存在的影片。骗徒甚至可能让来电显示成您认识且信任的号码或伪冒您的认识的声音以要求将资金转移到另一个账户。此被称为改号欺诈，其对话内容听起来可能非常真实可信，诈骗者甚至可能已经掌握了一些有关您的个人资讯，如账户号码或地址。如果您觉得有任何不妥，或察觉有异，请不要犹疑，立即挂断电话。您可以反过来致电您所知的机构电话号码，例如您银行卡背面的电话号码，以核实来电的真伪。

但请留意，骗徒可能继续保持通话线路连通，甚至伪造拨号的音效，让您误以为真。因此，请使用另一部手机，或相隔至少30秒后才致电。
常见的例子包括：

- 「您的银行」通知您的账户出现风险，需要将您的资金转移到另一个账户，以确保安全。
- 「您的银行」需要您的协助来调查诈欺事件。
- 您的网络或电讯供应商致电给您，替您解决您从没有报告过的问题。

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

深度伪造技术

深度伪造技术是利用人工智慧来模仿个人的外表和声音再合成为影片，从而冒充高层主管等高级管理人员。深度伪造技术可以透过多种管道传递，包括：语音讯息、电话或视讯通话。

深度伪造的语音和视讯可以令人容易信服，通常这些讯息的语气较为紧急，并要求提供敏感讯息，或会提出在协议之外的要求。

辨识深度造假需要注意以下几点：

- 眨眼— 在深度伪造技术下眨眼频率异常或看起来不自然
- 眼镜产生反光— 在深度伪造技术下通常无法完美呈现光照的自然物理特性
- 面部表情— 在深度伪造技术下面部表情可能过于僵硬
- 口型与说话不一致— 在深度伪造技术下说话口型可能有差异
- 渲染效果不足— 透过深度伪造技术，可能显示出奇怪的牙齿和珠宝可能会发出奇异的光芒
- 边缘模糊— 在深度伪造技术下脸部周围可能有闪烁的边缘
- 作出提问— 如对视讯通话有怀疑，作出提问测试对方身份真伪

入侵账户欺诈

骗徒可能以伪冒的电话号码致电给您，例如显示为恆生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，会引导您进行您所预期的流程，例如验证程序，以搏取您的信任。

接着，他们将以各种方法来骗取您的安全资讯，例如使用者名称、密码、安全代码。骗徒随后可以使用这些资讯，成功入侵您的账户，并将您的资金转走。

请谨记：

- 恒生不会要求您提供卡片PIN码、密码或安全代码。
- 不要向任何人透露安全代码。
- 恒生绝不会要求您将资金转移到任何安全账户。

防止诈骗

降低诈骗风险

每家企业都可以采取一些措施以降低诈骗风险。这些措施既不复杂，亦无需花耗大量成本。

- 评估您的业务，在最易受诈骗威胁的部份提高警觉。
- 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，任何新的受款人或账户的详细资料都需要经过核实。
- 对任何异常或不合理的请求，必须作出进一步的查询。
- 接下来的部分，将为负责付款的人员提供更详细的指引。

确认电邮地址

骗徒会伪冒为可信赖的人士。

- 如果发件人的名字相当熟悉（您认识或经常通信来往的人），请确认电邮地址是否相符。
- 如果发送人为同事，其电邮地址应列在公司的电邮件目录上（如有）。
- 确认网域名称的拼写是否正确。诈骗者经常会创建与真实域名非常相似的假域名，并更改一个或两个字母，务求令收件人不容易察觉。例如：J@rnbusiness.com 及 J@mbusiness.com。
- 请注意，电邮显示的名称可能与实际发件人的电邮地址不符。

仔细审查电邮

声称紧急情况更要警惕。

- 如果任何与付款事宜相关的电邮，使用了紧急的语气，或以没有回电选项为理由，则应视为可疑电邮。
- 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邮应加倍警惕，特别是那些载有连结或附件的电邮。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邮。
- 如果您收到不寻常的电邮，且/或不认识寄件人，请勿点击电邮内的连结或打开附件。

核实新收款人或账户的资料变更

请使用可靠的联络方式向对方查证。

- 在可行的情况下，请尝试与您相识的人联络。例如，如果公司内部人员要求资料变更，请直接致电该人员以作确认。如果变更要求来自供应商，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。

- 当您遇到可疑电话、电邮或网路卖家等情况时，您可以透过一站式诈骗陷阱搜寻器「防骗视伏器」手机APP ，输入平台帐户名称或号码、收款帐号、电话号码、电邮地址和网址等，以评估诈骗及网络安全风险。

防止诈骗

任何类型的企业均有机会遭受不同形式的欺诈幸而，您可以采取一些措施来让您的企业免受诈骗和网路犯罪的威胁。以下是一些可以帮助您降低企业内部诈骗风险的建议清单。

建议

制定及落实有关汇款的保安机制

防范欺诈的关键在于确保所有款项都经过充份的验证才付出。因此，企业应定立机制防止汇款团队在未经充份验证的情况下，授权新的或被要求变更的付款。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。

鼓勵員工三思而後點擊

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。

检查清单：高层管理人员

最有效抵御诈骗的方法，就是防范于未然。以下检查清单可为您提供一些实用建议，助您保护企业的网络安全

- ☐ 对于全新或经过修订的付款指示，贵公司有否订立验证机制？员工是否知道如何取得已知联络人的资料？
- ☐ 贵公司有否订立付款指示的保安机制？包括如何提出付款指示、由谁审核、以哪种方式支付，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？
- ☐ 贵公司有考虑应用双重验证机制及其可行性？
- ☐ 假如发生欺诈付款时，您的员工知道如何应对和处理吗？
- ☐ 对于欺诈攻击，例如电邮地址遭到入侵，贵公司有否制订应对措施？
- ☐ 您有定期与提交付款指示的相关人员讨论诈骗的潜在风险？

恒生銀行 HANG SENG BANK

检查清单之二：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，并培养对诈骗有警觉性的企业文化。

☐ **确认电邮地址的真伪**

如果电邮发件人的名字相当熟悉（您认识或经常通信来往的人），请确认电邮地址是否相符。

如果发送人为同事，其电邮地址应列在公司电子邮件目录上（如有）。此外，请确认网域名称的拼写是否正确，亦应留意诈骗者经常会创建与真实域名非常相似的假域名，但会修改一个或两个字母，务求令收件人不容易察觉。例如：J@rnbusiness.com 及 J@mbusiness.com。最后，请仔细检查电邮显示的名称，可能与实际发件人的电邮地址不符。

☐ **仔细审查电邮**

如果任何与付款事宜相关的电邮，使用了紧急的语气，或以没有回电选项为理由，则应视为可疑电邮。一些钓鱼邮件写得相当糟糕，即使拼写正确，也可能含有文法错误。对从外部发送过来的电邮应加位倍警惕，特别是那些包含连结或附件的电邮。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邮。如果您收到不寻常的电邮，且/或不认识寄件人，请勿点击电邮内的连结或打开附件。

☐ **核实新收款人或账户的资料变更**

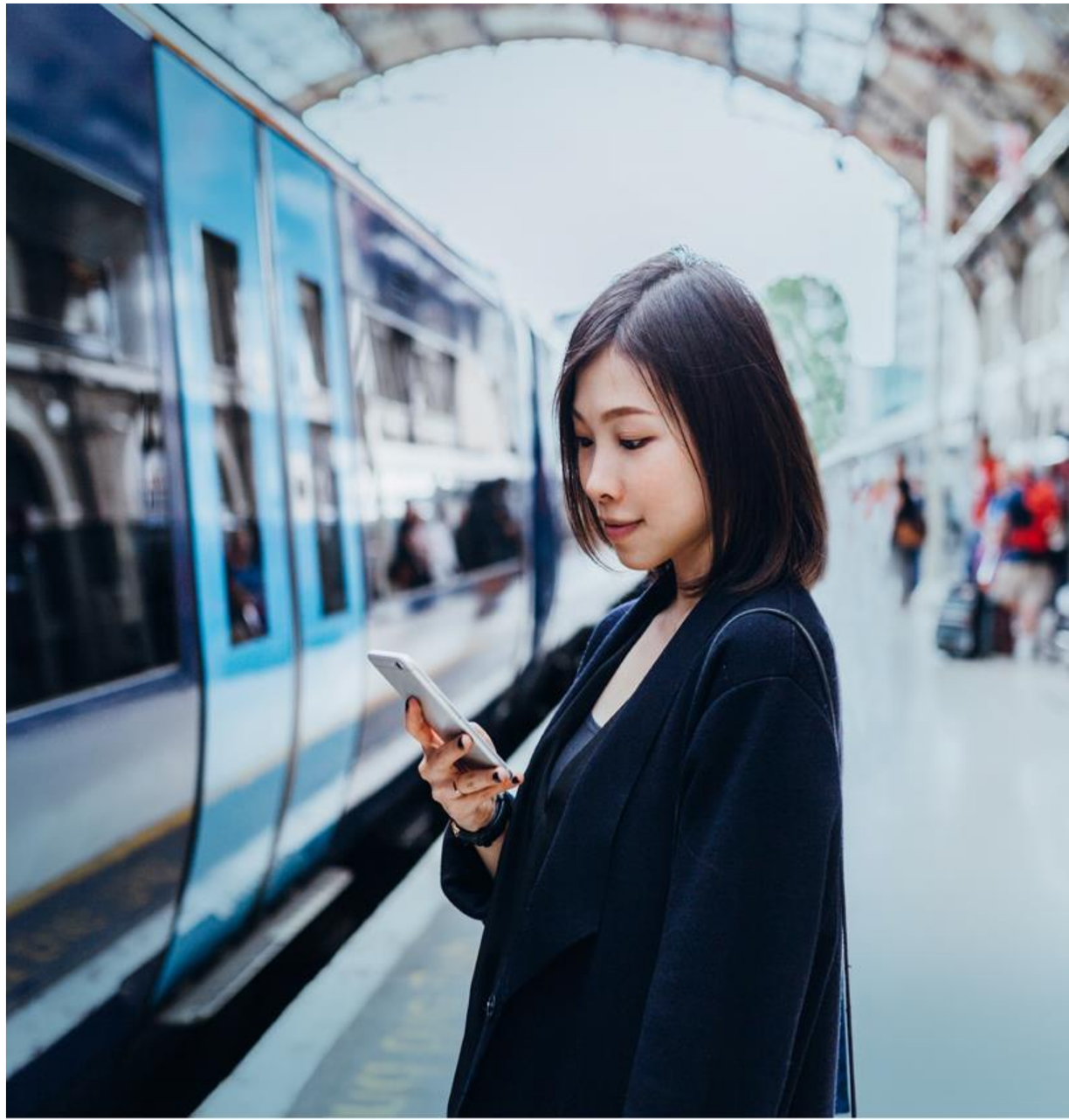
在可行的情况下，请使用可靠的联络方式向对方查证，并请尝试与您相识的人确认。例如，如果变更请求来自公司内部人员，请直接致电该人员以作确认。如果来自供应商，请致电与您经常联络的人员以作确认。请勿回覆电邮或使用电邮中的联络方式。一般情况下，网络不法分子在获得登入账户权限后，会向账户联络清单上的人士发送钓鱼邮件。这代表着即使电邮的内容相当可疑，您仍可能会因为电邮地址正确无误，而认为真的是由该寄件人发出。此时，您应致电该寄件人，既可以确认电邮中的要求，亦可提醒他们的电邮账户或已遭入侵。

☐ **透过「防骗视伏器」评估检查诈骗和网路安全风险**

当您遇到可疑电话、电邮或网路卖家等情况时，您可以透过「防骗视伏器」输入平台帐户名称或号码、收款帐户、电话号码、电子邮件地址、网址等，以评估诈骗风险和网路安全。

我们应评估所收到的请求是否合理？有没有异常的地方？

假如遭受诈骗应如何应对



如果您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减至最低，同时亦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），并须立即联络银行，发出退款指示。因为资金转移速度非常快，一旦被转移，退款程序便会更困难。
- 向有关当局举报诈骗个案。
- 查看您的财务记录，以辨别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，包括电邮、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。

向恒生举报诈骗

如您遇到以下情况并怀疑受骗

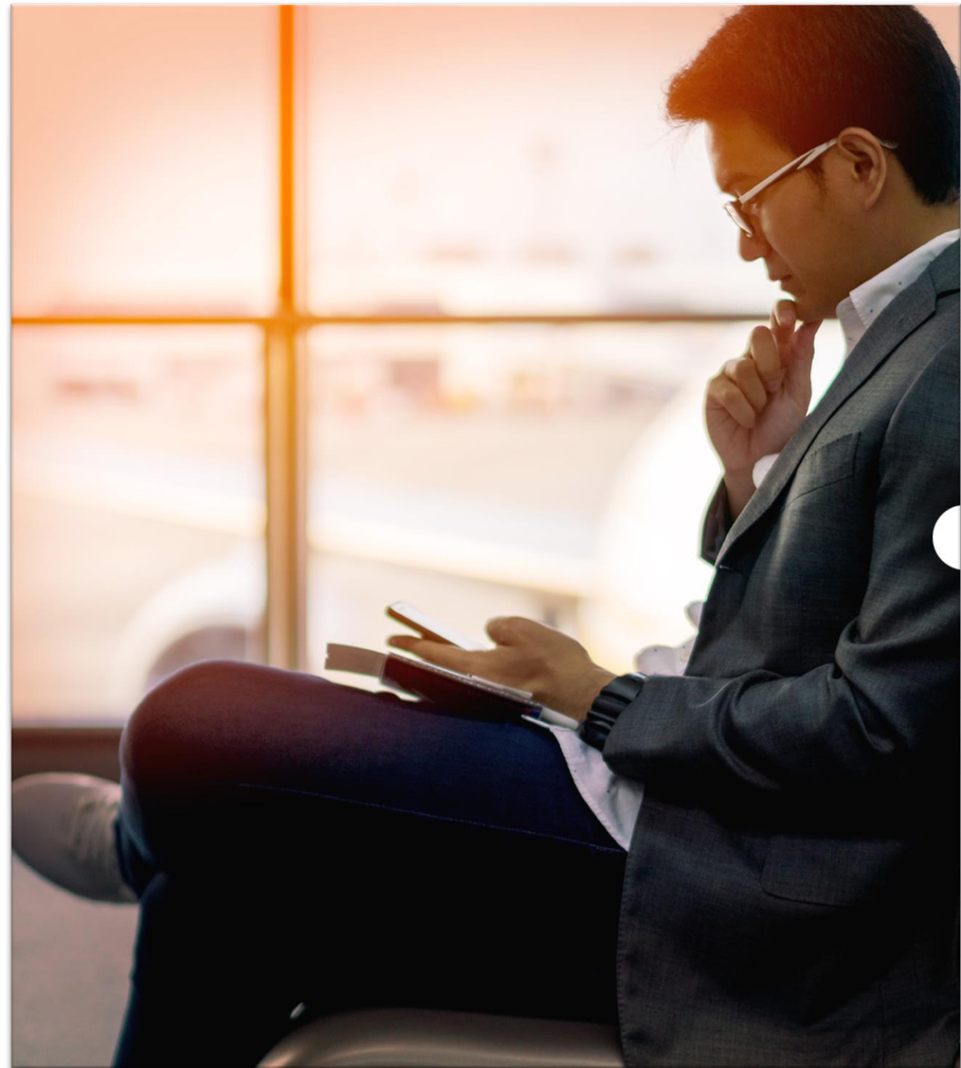
1. 未经您授权的诈骗性转账或账单支付;
2. 您之前授权进行了银行转账或账单支付，但现在认为自己已经成为诈骗的受害者

请即透过以下方式与我们联络，我们将24小时全天候为您提供协助：

- 如果您身处香港，请致电 (852) 2198 8000

- 如果您身处中国，请致电 4001 20 8288

我们亦建议你请前往就近的警署或于香港警务处电子报案中心(police.gov.hk)报案。如遇到紧急事故，请立即致电（999）报警求助。请保留报案号码，并致电上文提到的方式通知我们。



如果您遭受网络攻击，请采取以下措施：

- 关闭所有受影响设备的网络连线，以防止恶意软件散布或未经授权的入侵。
- 更改所有受影响账户的密码，包括电邮、网络和其他可能泄露了资料的账户。
- 聘用信誉良好的网络保安公司，对您的系统进行全面检查，以发掘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资料。
- 确定攻击来源，并采取措施，防止未来再次遭受类似的攻击。

术语概览

诈骗和网路安全术语须知

- 防毒软体 - 用于预防、侦测，甚至移除恶意软体的电脑程式。
- 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作公务用途。
- 常见漏洞与揭露（CVE） - 罗列已发现资安弱点及漏洞的清单，并提供独有的ID编号、描述和参考资料以便供公众查阅。
- 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 - 对电脑系统、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《滥用电脑法》（1990年）」。
- 暗网 - 网路的其中一部分，但无法在搜寻器搜索出来，仅能透过特殊权限或软体访问。
- 数码足迹 - 使用网路后留下的数据踪迹，可能包括被动信息，如存储的Cookie，或者被主动在网络上发表的资讯，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，例如储存在硬碟中的数据，亦可以是传输中的数据，例如透过 HTTPS 从您的网页浏览器传送到银行伺服器的资料。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，让不法份子得物无所用。
- 防火墙 - 根据特定规则，监控网路进出流量的网路安全系统。
- 骇客 — 专门从事电脑网路攻击的人士。黑帽骇客进行恶意攻击，而白帽骇客则进行有助于网路防御的行动。
- 恶意软体— 以达成不法或恶意目标的程式，涵盖多个方面，例如提供远端存取、载入或植入其他恶意程式、窃取银行资讯、加密并拒绝存取资料，或盗用设备的运算能力。
- 安装补丁 — 安装修补程式以更新现有软体或硬体，修复已发现错误和漏洞的过程。
- 渗透测试（pen testing） - 机构利用骇客的攻击手段来检测自身网络的安全性，通常由「红队」或专业的白帽骇客团队负责。

- 钓鱼 - 通常透过电子邮件欺骗收件人泄露敏感资料、点击恶意连结和/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。
- 勒索软体 - 封锁或限制使用者存取资料的恶意软体，并要求受害者支付赎金才能解除限制。
- 短讯钓鱼 — 透过短讯/简讯传送的钓鱼讯息。
- 社交工程 — 操控他人的心理而作出某种行为，通常用于骗取个人资料。
- 鱼叉式网路钓鱼 — 针对特定人士或群体所发出的钓鱼讯息。
- 特洛伊木马 — 伪装成看似无害的档案或程式，让受害者以为可安心开启。特洛伊木马十分常见，通常透过钓鱼邮件传送，或者由其他称为「载体」的恶意软体传送。
- 双重要素验证（2FA） — 一种要求用户提供两种身分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）。
- 虚拟私人网路（VPN） — 允许在公共基础设施上建立安全私人的连线，最初由机构开发，以对访问内部网络资源，例如电邮伺服器或共享文件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伺服器的加密连线，并使用该伺服器连接到其他互联网资源。
- 语音钓鱼 — 透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体通常被称为零日漏洞攻击。

恒生銀行
HANG SENG BANK

Thank you!