恒生銀行
HANG SENG BANK

恒生防诈骗指南

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

近年来，诈骗已成为企业最常面临的威胁之一。

稍有不慎，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，本指南旨在帮助您和您的员工及早辨识诈骗危机，作出有效的预防措施。如您不幸成为受害者时，也可采取正确的应对措施。

高达1.02万亿美元

根据非营利组织全球反诈骗联盟（GASA）和数据服务提供商ScamAdviser发布的2023年报告，在过去的这一年，全球诈骗案共造成了约1.02万亿美元（约合人民币7.34万亿元）的损失，相当于全球GDP的1.05%。

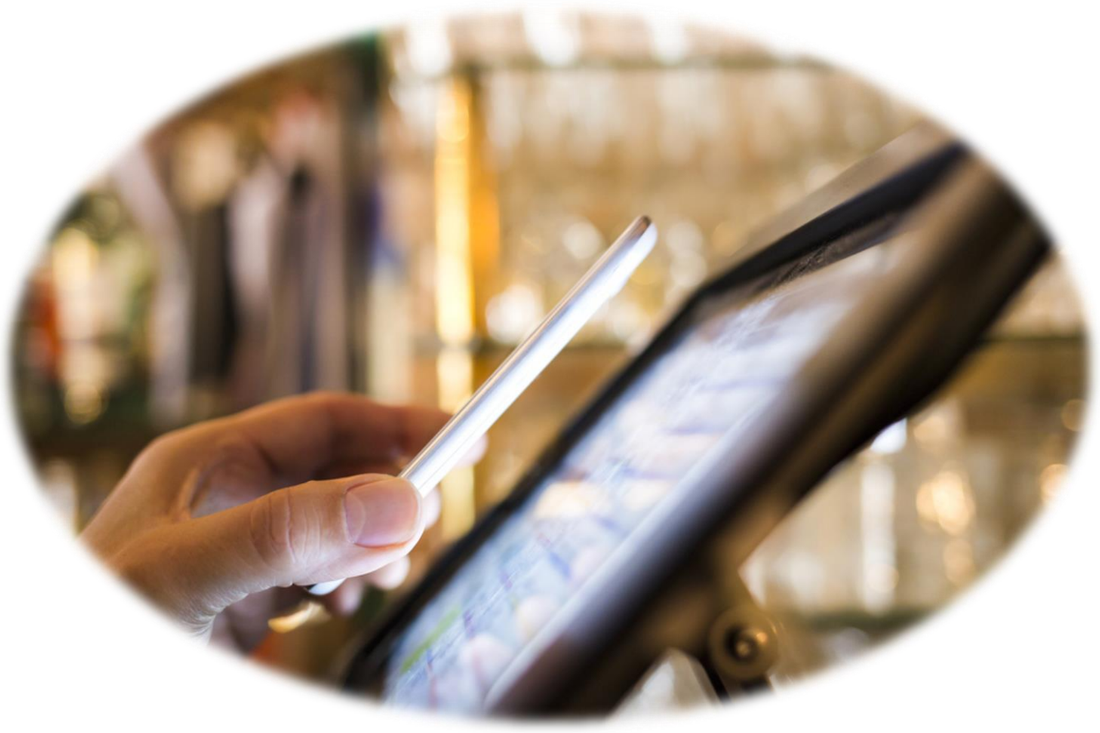
数据源：时代周报

本指南将帮助您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。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，可供管理及处理交易的支付团队进行参考。

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您信任的联络人或者您的银行，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，告知您收款银行的详细信息已更改，并将更新后的信息提供给您要求您付款。

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，是指诈骗者假冒成您的银行或其他可信任的机构来进行电话诈骗。以如今的人工智能技术（例如：深度伪造技术），骗徒能从图像截取你的容貌伪造成影片。此外，深度伪造技术还可通过声音模仿，只需截取你五秒钟的对话，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。

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您的个人信息，如账号号码或地址。如果您觉得有任何不妥，或察觉异常，请不要犹疑，立即挂断电话。您可以反过来致电您知道的机构电话号码，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，骗徒可能还继续保持着通话线路的连通，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秒后再致电。
常见的例子包括：

- “您的银行”通知您的账号出现风险，需要将您的资金转移到另一个账号，以确保安全。
- “您的银行”需要您的协助来调查欺诈事件。
- 您的网络服务商或通信运营商致电给您，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。

其他常见的诈骗攻击方式

深度伪造技术

深度伪造技术是利用人工智能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。深度伪造技术可以通过多种途径传递，包括：语音信息、电话或视频通话。

深度伪造的语音和视频可以令人容易信服，通常这些信息的语气较为紧急，并要求提供敏感信息，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-通过深度伪造技术，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-如对视频通话有怀疑，做出提问测试对方身份真伪

入侵账号欺诈

骗徒可能以伪冒的电话号码致电给您，例如显示为恒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，会引导您操作您所预期的流程，例如验证程序，以博取您的信任。
接着，他们将以各种方法来骗取您的安全信息，例如用户名称、密码、安全代码。骗徒随后可以使用这些信息，成功入侵您的账号，转走资金。

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号。

防止诈骗

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。

- 评估您的业务，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（您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。
- 如果您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，请尝试与您认识的人联络。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，请致电与您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，您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，您应致电该发件人，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，您可以采取一些措施来让您的企业免受诈骗和网络犯罪的威胁。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。当您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/网络攻击时应采取的措施

如果您或您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。

请尽快联络您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。以下自检清单可为您提供一些实用的建议，帮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，您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？
- [ ] 您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（您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**

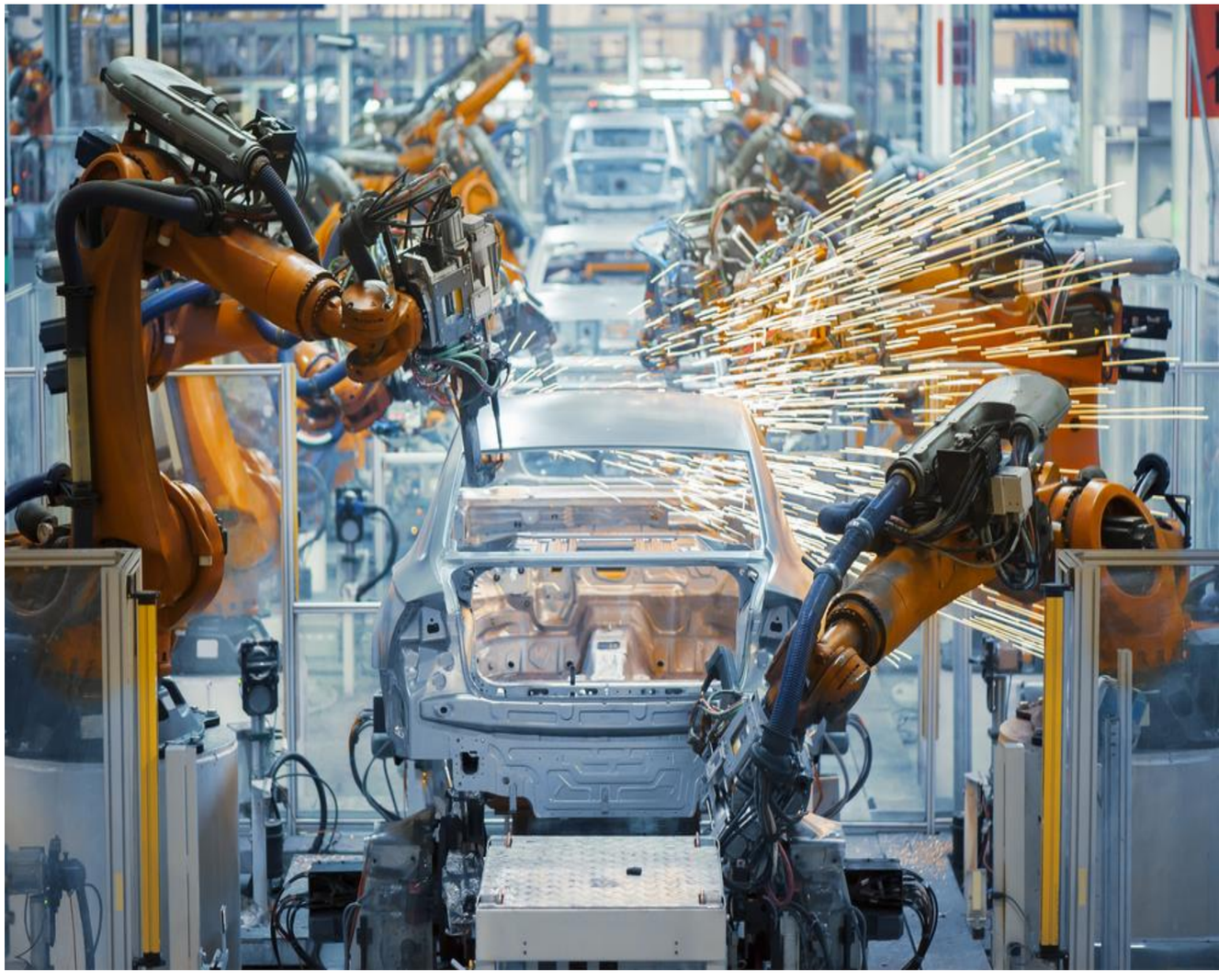
任何与付款事宜相关的电子邮件，如若使用了紧急语气，或以没有回电选项为借口，则应视为可疑电子邮件。一些钓鱼邮件写得相当糟糕，即使拼写正确，也可能含有语法错误。对从外部发送过来的电子邮件应加倍警惕，特别是那些包含了链接或附件的电子邮件。请注意，生成式人工智能使得骗徒更容易杜撰更真实可信的恶意电子邮件。如果您收到非正常的电子邮件，且/或不认识发件人，**请勿点击电子邮件内的链接或打开附件。**

☐ **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，并请尝试与您认识的人确认。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，请致电与您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，您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，您应致电该发件人，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



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。**
- **查看您的财务记录**，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。**

向恒生举报诈骗

如您怀疑有未经您授权的诈骗性转账或账单支付；或如果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，或您怀疑您的个人资料已经被泄露，建议拨打公司客户服务热线与我们联络:

中国内地可拨打： 800-830-8008

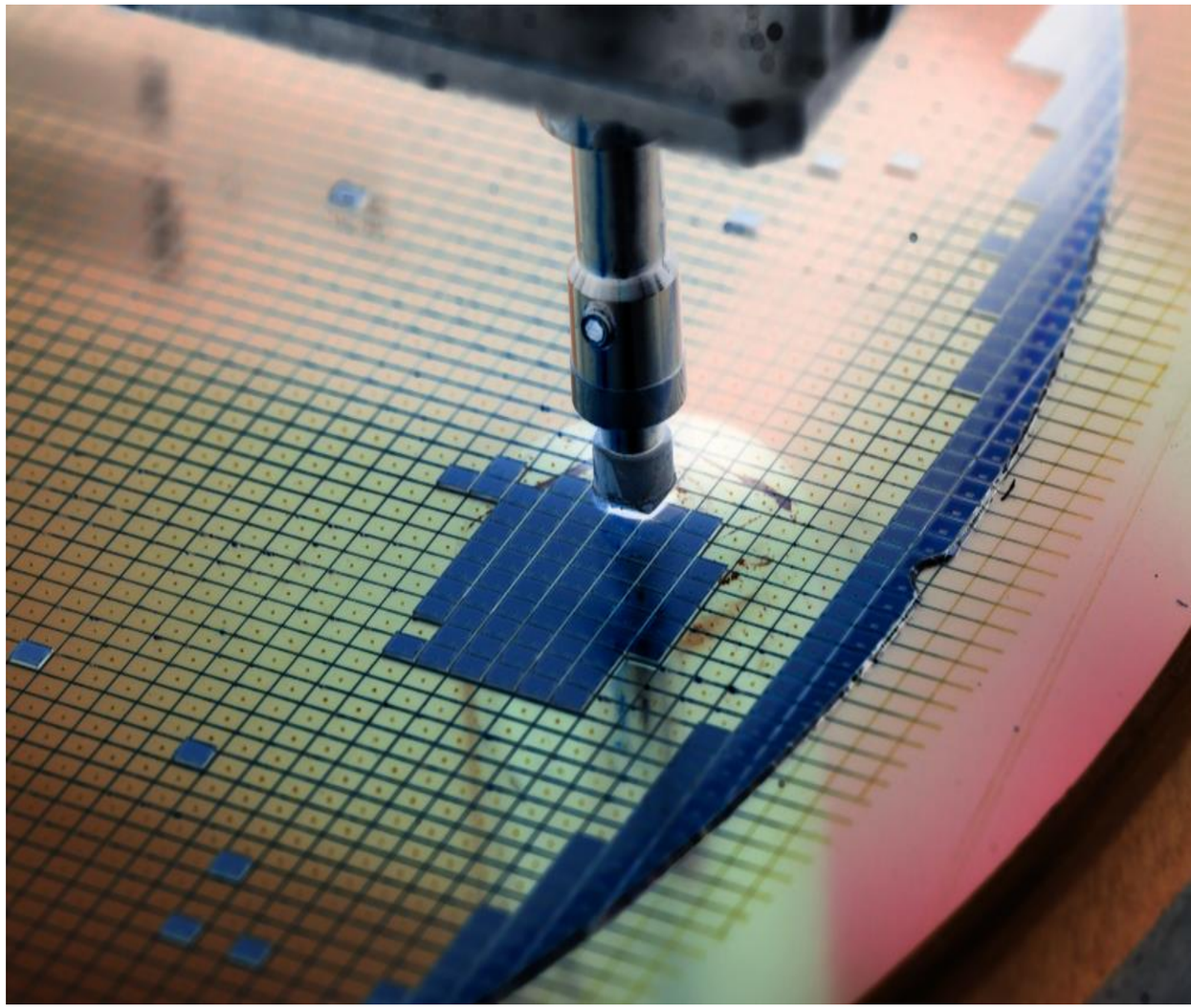
非中国地区可拨打，拨打前请加区号 +86： 400-830-8008

我们也建议您请前往就近的的警察局。如遇到紧急事故，请立即致电（110）报警求助。请保留报案号码，并致电上文中提到的方式通知我们。并鼓励您安装国家反诈中心APP。

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，对您的系统进行**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 从您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。

恒生銀行
HANG SENG BANK

谢谢！