

保安资讯

本页刊载南洋商业银行有限公司（「本行」）有关的电子银行服务的保安资讯。电子银行服务指透过互联网、无线网络、自动柜员机、电话网络或其他电子网络、终端机或设备提供的银行服务，包括但不限于本行网上银行（个人及企业）、手机银行（个人及企业）、南商 e+ 流动应用程序（「南商 e+」）、电话银行、自助服务及微信官号等。

最新 / 重要保安资讯

提防流动装置恶意软件（Malware）骗案

识别恶意软件

- 恶意软件会在未经用户同意下，入侵、破坏其流动或计算机装置系统，或从中获取数据。恶意软件包含间谍软件、计算机病毒和特洛伊木马程序。
- 间谍软件是一种在未经用户允许下安装的软件，它会隐藏不诚实的目的去监察和记录用户数据/网上行为，及收集和传送撷取得来的数据（如身分识别数据，包括用户名称、密码及信用卡号码等）给未经授权的第三方而从中获取利益。
- 病毒可能藏有具破坏性的编码，能潜进某系统之多种程序、数据文件或设备，以及扩散到同一网络下的不同系统，最终引致受影响的装置故障和数据损失。
- 另一种恶意软件为特洛伊木马程序，它会伪装成看似无害的程序，但能够在用户不知情下控制其装置和进行不法活动。

如何妥善应对

- 客户应透过认可的官方软件应用商店（如 Google Play，App Store 及华为香港应用市场等）搜寻「NCB」免费下载南商个人手机银行（「NCB 南洋商业银行」）、企业手机银行（「NCB 企业版手机银行」）及南商 e+ 流动应用程序（「南商 e+」）。
- 保持装置的配置正确（例如不允许安装来自未知来源的应用程序等）。
- 安装应用程序前，仔细评估应用程序的请求权限，请勿随意授权第三方取得手机完整控制权或共享屏幕画面，如果发现可疑权限需求，切勿安装相关手机应用程序。

- 应在个人电脑安装防火墙软件及防电脑病毒软件，并且不时更新。
- 切勿用 Jailbreak（越狱）或 Root 机等手法改装流动装置或使用已被这些手法改装的流动装置以确保接驳电子银行服务装置安全和保密。
- 在任何情况都不应使用来历不明的应用程序。切勿点击不明短讯、电邮、网页或社交媒体内容中的连结或从这些连结下载任何档案。如发现任何可疑下载的程序，切勿尝试登入及停止操作。
- 客户应确保使用电子银行服务的设备不受到计算机病毒感染或不被未经授权的恶意、破坏性或损坏性程序代码进入以取得、使用或更改客户的密码、「生物认证」（例如：指纹、Face ID）或个人资料。
- 为保障客户账户安全及应对网络诈骗风险，本行已暂停手机银行（个人及企业）在流动装置的屏幕截图及录屏功能。同时，如本行识别到您的 Android 装置有潜在风险，例如：您的装置上安装了可疑应用程序，或已启用「辅助功能」/「无障碍功能」等相关辅助功能的应用程序；遇上此等情况，您的南商流动应用程序将有机会无法继续使用。本行建议即刻删除可疑应用程序，或关闭有关应用程序的相关辅助功能，以保障您的账户安全。

警惕诈骗来电、手机短讯、电邮

识别诈骗来电、手机短讯、电邮

- 来电者可能自称来自银行或其他金融机构，可能会邀请您申请个人贷款等金融服务，並以欺诈手段诱骗您提交个人资料或存入款项至指定账户以申请银行服务；或声称您的银行账户或银行卡出现异常，要求提供您的个人资料以核实身份或查核交易。
- 骗徒可能通过预先录制的语音消息来电，通知您银行户口出现异常，要求您透露敏感个人资料包括账户号码、用户名称及登入密码等，以让他们作出「调查」。他们亦可能假冒电讯公司、网上购物或支付平台客服，或是速递公司职员、本地和内地官员等身份，以不同理由要挟你提供个人资料，或将款项转到指定银行账户以骗取金钱。
- 在冒充过程中，骗徒可能相应提供了银行职员的资料（因为骗徒可以通过不法手段获得这些资料）或提供像真度极高的其冒充机构之员工证或名片，亦可能装作不畏惧身份核实，提供虚假的职员编号等数据，以图增加可信度。同时，伪冒来电通常通话音质较差，仿佛是长途电话来电。

如何妥善应对

- **诈骗电话安全提示**

- 客户应提高警觉，慎防伪冒银行的欺诈电话及语音消息来电。
 - 客户应注意不要向来电者提供任何敏感性的个人资料（包括登入密码和其他认证资料，如一次性密码、「保安编码器」或「流动保安编码器」所产生的一次性「保安编码」等）。如有疑问或曾向可疑第三者提供过个人资料，请致电本行 24 小时保安热线（852）2616 6628，并立即向警方报案（或致电香港警务处反诈骗协调中心的 24 小时咨询热线 18222，寻求警方协助）。
 - 请注意，本行绝不会透过电话、短讯或电邮收集您的敏感个人资料（包括登入密码和其他认证资料，如一次性密码、「保安编码器」或「流动保安编码器」所产生的一次性「保安编码」等），亦不会透过预录语音消息通知您银行户口出现异常。若收到自称是银行职员电话或语音消息请提高警惕。慎防伪冒银行的欺诈电话及语音消息来电。
 - 为保障客户利益，本行已经加入由通讯事务管理局办公室推出的「短讯发送人登记制」，为了帮助您更好识别本行已登记的发送人名称，请前往本行网页（本行网页>「关于南商」>「客户通知」>）阅览“有关南洋商业银行实行「短讯发送人登记制」通知”详情。
 - 当接到自称是电讯公司、网上购物或支付平台的客服，或是速递公司职员、本地和内地官员等的来电或讯息时，您可先在官方途径核实来电号码和对方身份，切勿急于向不明人士转账或透露个人资料。
- **接到可疑来电时您可采取的措施**
 - 客户应注意，本行职员致电客户时，将向客户提供包括且不限于以下信息：致电职员姓名、员工编号、联络电话，并提示客户可通过致电本行 24 小时保安热线（852）2616 6628 以核实来电者身份。
 - 当接到自称是本行职员的来电时，您可按对方提供的信息作初步判断。您可以进一步询问来电者所属的部门/分行名称和办公室号码，并确认他们是如何获得您的电话号码和账户信息的。如果来电者不愿意提供信息，请立即挂线。
 - 若您曾向或怀疑曾向伪冒来电者提供个人资料，请致电本行：（852）2616 6628，并向警方报案（或致电香港警务处反诈骗协调中心的 24 小时咨询热线 18222，寻求警方协助）。
 - 如果您向来电者提供了密码，请立即更改。
 - 如果您需要暂停网上银行账户服务，请致电本行：（852）2616 6628（如欲恢复网上银行账户服务，您可前往本行的任何一间分行重启相关服务）。
 - **您可以按以下途径核实来电者的身份：**
 - 拨打本行 24 小时保安热线（852）2616 6628（选择语言后按“9”）；或：

- 在本行网站 “联络我们 > 网上查询与保安问题 ” 上填写并提交表格，本行将于 1-2 个工作日内跟进；或：
- 亲临分行。

慎防网络钓鱼

识别「网络钓鱼」

- 「网络钓鱼」是一种常见的诈骗手法。骗徒会伪装成银行、网上付款服务供货商及网上购物平台，透过电子邮件、短讯或假冒网上购物平台内实时通讯方式，诱使对方提供敏感个人资料及认证因素（如登入密码、一次性密码等）。网络钓鱼电子邮件内亦可能包含恶意超链接、二维码或附件，引导对方至非法网站。一旦连接到仿冒网站，受害人通常会被要求输入个人资料或认证因素（如登入名称、账户号码、登入密码、一次性密码）。「网络钓鱼」网站会收集受害人输入的一切资料，骗徒利用该等资料盗取您账户金钱利益而令你招致损失。

如何妥善应对

- 本行不会透过第三者网站、第三者手机应用程序或以电邮、手机短讯、实时通讯或致电要求客户提供其个人资料及认证因素（如登入名称、账户号码、登入密码和其他认证资料，如一次性密码，「保安编码器」或「流动保安编码器」所产生的一次性「保安编码」等）。亦不会透过短讯或电邮超链接、二维码或附件，引导客户到本公司网站或流动应用程序进行交易。客户必须小心保管其个人资料及认证因素，如客户收到此请求，请即与本行联络。
- 为确保交易安全，客户应在浏览器网址栏内直接键入本行的网址以登入网上银行。切勿透过任电邮、短讯、二维码、互联网搜索器或社交网络平台提供的超链接，或非本公司认可的第三者网站或流动应用程序登入本公司的网上银行。如有怀疑、请立即停止操作，切勿输入任何资料，关闭窗口。
- 客户在登入电子银行服务时，请注意登入版面有否出现任何异常情况（例如：不正常的弹出版面、视窗运作缓慢、重复要求客户输入密码等）。切勿透过不明 Wi-Fi 或公用电脑登入网上银行。
- 在进行网上交易时，于输入认证因素进行交易验证前，请小心核对交易详情，例如：交易类别、交易金额及货币等，以确认是实际上进行之交易，不要盲目输入一次性密码。输入任何资料或进行交易前，须检视该网页地址是否真实与可信。如有查询，请立即与本行联络。
- 使用流动电话号码、电邮地址、FPS 标识符（FPS ID）或以二维码进行付款前，请小心核对付款详情，包括收款人名称。如有任何怀疑，请先向收款人确认。

其他重要保安资讯

- 客户不应透过第三者网站、第三者手机应用程序、电邮、短讯或实时通讯讯息中的超链接、二维码或附件登入网上/手机银行或提供任何敏感性的个人资料。为确保交易安全，客户应在浏览器网址栏内直接键入本行的网址以登入网上银行，或从官方认可的应用商店下载和安装應用程式以登入手机银行服务。
- 客户应注意就电子银行服务的保安问题应负的责任，包括及时阅览及遵守本行《服务条款》及为保障客户而不时列明的有关保安措施。
- 客户有责任采取合理步骤，确保接驳电子银行服务所用的任何装置（如个人计算机、发出一次性密码的保安装置和储存数码证书的智能卡）或认证因素（如个人密码及认证令牌）安全和保密，包括但不限于：
 - 销毁印有其密码的文件；
 - 请留意采用生物特征、软令牌或装置绑定作为进行相关交易的认证因素之一所涉及的风险（认证因素遗失、被窃、资料外泄或遭未经授权使用），以及确保装置和认证因素安全的相关保护措施。如发现可疑装置，以及在发现其卡或账户有异常或可疑交易后，应尽快通知本行。
 - 切勿让任何其他人士知道及使用其认证因素；
 - 绝对不可将其密码写在任何使用电子银行服务所需的装置之上，或其他经常与此等装置放在一起或放在附近的物件上；
 - 不应直接写下或记录密码，而不加掩藏；
 - 在发现其账户有异常或可疑交易/活动后，请即致电本行 24 小时保安热线（852）2616 6628 申报相关异常情况并要求实时暂停网上银行账户服务；及
 - 需要确保其在本行登记用于接收本行重要通知的联络方式（例如用于网上付款的短讯及电邮通知）是最新且真实有效的，以便有关通知能够及时向客户发送。
- 如客户发觉或相信其接驳电子银行服务所用的认证因素或装置遭泄露、遗失或被盗用，又或者其账户曾录得未经授权交易/活动，客户必须在合理可行的情况下尽快通知本行。
- 除非客户作出欺诈或严重疏忽行为，如未能妥善保管接驳电子银行服务的装置或认证因素，否则客户无须对因经其账户进行的任何未经授权交易而蒙受的直接损失负责。此点规定不适用于下文“自动柜员机及提款卡的安全资讯”所载有关透过卡进行未经授权交易的规定。

- 若损失是因客户的欺诈行为而引致，客户将要承担所有损失。若损失是因客户严重疏忽（可能包括在知情情况下容许他人使用其装置或认证因素），或者因客户在发觉或相信其接驳电子银行服务所用的认证因素或装置遭泄露、遗失或被盗用，又或其账户曾录得未经授权交易后，未能在合理切实可行的情况下尽快通知本行而引致，客户亦可能要承担所有损失。客户如未能遵守本文所载的保障措施而导致损失，此点的规定亦可能适用。
- 客户在登入电子银行服务时，请注意登入版面有否出现任何异常情况（例如：不正常的弹出版面、视窗运作缓慢、重复要求客户输入密码等）。客户如有任何怀疑，切勿按照可疑网页上的指示操作或输入任何资料，并请即终止电子银行服务的操作。如有查询，请与本行联络。
- 客户必须小心保管其个人资料（包括个人生物认证资料）。本行不会以电邮、手机短讯、实时通讯或致电要求客户提供其个人资料，如用户名称、密码、一次性密码或其他账户资料。
- 在进行交易时，于输入一次性密码进行交易验证前，请小心核对交易详情，例如：交易类别、交易金额及货币等，以确认是实际上进行之交易。如有查询，请立即与本行联络。
- 客户应警惕涉及将卡绑定到移动支付服务的银行卡诈骗，以保护其支付卡、卡信息和身份验证相关的资料。
- 客户可能需要承担未能妥善保护其实体卡、卡信息和身份验证信息的后果，特别是因忽视银行卡前和卡后交易相关通知而产生的后果。