

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：

- 客户应透过官方软件应用商店(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+」)。
- 客户应只从官方认可的应用商店下载和安装由可信任开发商提供的已验证的应用程序，并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)。
- 在安装应用程序前，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。
- 切勿用 Jailbreak (越狱) 或 Root 机等手法改装流动装置。
- 在任何情况都不应使用来历不明的应用程序。不要浏览可疑网站，或从这些网站下载任何档案。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 Android 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。

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，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。
- 如客户需要核实自称为本行职员之来电者身份，请拨打本行 24 小时保安热线 (852) 2616 6628(选择语言后按“9”)。
- 客户应注意不要向来电者提供任何敏感性的个人资料(包括登入密码及一次性密码等)。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)。

其他重要保安资讯：

- 为保障您的网上银行账户安全，于网上银行或手机银行登入版面增加验证码。客户在登入网上银行或手机银行服务时，除需要输入网上银行号码/用户名称、密码外，需同时输入「验证码」。
- 为保障您的网上银行账户安全，客户在登入南商 e+ 查看账户信息或更新开户申请资料时，除需要输入「短讯一次性密码」外，还需输入「南商 e+ 登录密码」。

- 为了进一步加强互联网交易安全，客户于网上银行及手机银行办理指定交易时，必须使用「双重认证」及以指定方式接收交易通知，才可继续办理有关交易。有关网上及手机使用双重认证办理指定交易的详情，请浏览本行网页：「电子银行服务 > 双重认证」。
- 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；
 - 切勿让任何其他人士使用其认证因素；
 - 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)。
- 客户在登入电子银行服务时，本行绝不需要客户在保安编码器上输入任何资料以产生登入编码。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。

诈骗电话安全提示

什么是诈骗电话，如何识别诈骗电话

- 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。
- 请注意，本行绝不会通过电话或电邮收集您的敏感个人资料(包括登入密码及一次性密码等)，亦不会透过预录语音消息通知您银行账户出现异常。如果来电者要求您提供密码等敏感信息，请提高警惕。

接到可疑来电时您可以采取的措施

- 客户应注意，本行职员致电客户时，会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、核实来电者身份的方法。
- 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）。

本行采取哪些措施帮助您核实来电者的身份

- 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。

网上保安提示及资讯

我们为您提供的保障

- 本行采用国际认可的 Transport Layer Security (「TLS」)加密技术，保障资料传送的安全，防止第三者盗取客户的资料。
- 网页服务器设有防火墙，防止未经授权人士进入本行的系统。
- 本行系统会记录客户的登入次数。如客户连续多次输入错误的登入密码，有关网上银行服务会被即时暂停。
- 本行于网上银行(个人及企业)为客户提供操作日志查询功能；例如客户可登入网上银行后查阅登入记录（个人网上银行: 我的账户 > 更多服务 > 日志查询 > 登入登出；或企业网上银行：客户服务 > 日志查询），包括登入时间、位置信息、和浏览器信息，以便及时发现潜在异常活动。
- 如客户正使用的网上服务静止（即没有任何操作指示）了一段指定时间，服务将被自动终止联机，以防止任何未经授权的交易。
- 如客户在已经登入网上银行的情况下登入同一账户的手机银行，则网上银行服务将被自动终止联机。

- 本行为客户于网上银行/手机银行服务提供「流动保安编码」及「保安编码器」作为双重认证工具；部份指定交易服务会为客户提供以手机短讯形式发出的一次性短讯密码进行验证。
- 为确保您可以收到本行的通知信息以保障您的网上交易安全，若您的通讯资料（如电邮地址或通讯地址）有所变更，请登入网上银行(设定 > 更新客户资料) 并使用双重认证以更新个人资料。若您需更新手机号码等通讯资料，请前往任何一间分行办理。

安全凭证

本行采用扩展验证 SSL 证书，让客户可透过检视浏览器的地址栏，核定所进入的网页是否本行的真确网页。

Microsoft Internet Explorer 版本 9 或以上浏览器的地址栏为绿色，是扩展验证 SSL 的其中一个保安特征。如客户选用 Microsoft Internet Explorer，亦可在网上银行的登入版面上按「安全锁」标志，以查阅证书内容，包括其有效日期及以下资料。请注意，各项资料的显示方式会因不同浏览器版本而有所差异。有关扩展验证 SSL 证书详情，请浏览证书发行者 Sectigo 的网页。

 <p>个人网上银行 发给：pnb.ncb.com.hk 发行者：Sectigo RSA Extended Validation Server CA</p>	 <p>企业网上银行 发给：cpb.ncb.com.hk 发行者：Sectigo RSA Extended Validation Server CA</p>
--	---

符合基本保安要求的浏览器

为确保客户资料安全，请安装建议的浏览器版本登入网上银行服务：

个人网上银行	企业网上银行
<ul style="list-style-type: none"> ● Microsoft Edge (版本 14 或以上) ● Mozilla Firefox (版本 72 或以上) ● Apple Safari (版本 10 或以上) ● Google Chrome (版本 80 或以上) 	<ul style="list-style-type: none"> ● Google Chrome (版本 80 或以上) ● Mozilla Firefox (版本 72 或以上) ● Microsoft Edge (版本 14 或以上) ● Apple Safari (版本 10 或以上)

网上保安提示

1. 防范伪造网站

请保持警觉并注意任何试图冒充本行网址的伪造网站。客户必须完全确定登入本行网站，否则不应提供任何相关的网上服务资料。

2. 欺诈电邮

请注意，计算机病毒、特洛伊软件及黑客程序可透过电子邮件传播，蠕虫病毒更可将病毒复制及发送至电邮地址簿上各收件人。因此，客户不应开启并应实时删除来历不明的电子邮件，亦不要透过电子邮件或短讯提供的超链接或二维码登入网上服务。如需开启电子邮件内的附件，亦应先进行病毒扫描。此外，客户应提高警觉，以防骗徒藉电邮进行不法活动。

如涉及汇款交易，请勿单靠电邮往来办理。客户应使用其他渠道(例如：电话、传真等)确认交易内容及收款人资料后才完成汇款。

欺诈电邮例子一：商业层面电邮诈骗

骗徒对一名海外买家及其服务供货商在过去数月的电邮往来进行监视。当该名黑客了解了有关交易详情后，便利用与服务供货商名字相近的假电邮地址，指示买家将款项汇往一欺诈账户。

欺诈电邮例子二：冒领遗产诈骗

骗徒发出电邮并声称作为银行职员，指其一名已去世的客户留下巨额定期存款，无人认领。骗徒邀请收件人讹称为去世客户的亲属以领取存款。如收件人同意合作，骗徒便要求收件人先缴付款项，以支付文件费用。最终收件人被骗去有关款项。


欺诈电邮例子三：未经授权的设备绑定及资金转账

骗徒冒认银行发出嵌入超链接的欺诈电邮，客户输入其电子银行账户资料和短信一次性密码。诈骗者利用银行的移动应用程序，使用有关资料和一次性密码将其移动设备连接到受害者的银行账户。尽管设备绑定有延迟执行期，但客户仍被欺骗，通过提供帮助（例如输入另一个短信一次性密码）来帮助欺诈者在延迟期后激活其设备。诈骗者可以成功登入客户的银行账户，并利用其在未经授权的情况下将资金转移到外国银行账户。

3. 欺诈实时通讯讯息

客户务请提高警惕，留意任何冒充本行或冒充银行职员发出的诈骗性实时通讯讯息。这些消息通常会诱使接收者提供个人或账户详细信息，以进行身份识别或参与投资计划。客户不应回复这些消息、点击任何可疑链接、下载任何可疑文件或提供任何信息。

4. 浏览器中间人攻击

近日发现有个别企业客户的计算机怀疑受特洛伊木马程序攻击，在登入企业网上银行时，计算机显示一个虚假网页，除要求客户输入登入名称、密码外，并同时要求客户输入由「保安编码器」发出的一次性「交易确认编码」。

为保障客户使用网上银行服务的安全性，请客户经常保持警觉，在登入网上银行时，应注意登入版面有否出现任何异常情况(例如有不寻常的窗口弹出，及/或计算机操作出现异常缓慢的情况等)，如有怀疑，切勿按照可疑网页上的指示操作输入任何资料，并请即关闭窗口。本行在客户进行「指定交易」时，才会要求客户输入由「保安编码器」发出的一次性「交易确认编码」；在登入网上银行时，本行不会要求客户输入该一次性「交易确认编码」。(请参阅以下网上银行登入版面)

本行藉此机会提示客户应在其个人计算机安装防火墙软件及防计算机病毒软件，并且不时更新，同时应避免进入可疑网站或从该等网站下载软件，亦不要随便开启来历不明的电邮内的附件。切勿点击或打开可疑或疑似银行发出之电子邮件中的附件或超链接。您可透过本行的网站 <http://www.ncb.com.hk> 或使用本行手机银行应用程序登入网上银行，切勿透过任何电子邮件、短讯或互联网搜索器提供的超链接登入网上服务。如有疑问，请联络本行，以核实银行是否确实发送了有关电子邮件。

个人网上银行登入版面



客户输入网上银行号码/用户名称、网上银行密码及验证码，然后按「登入」

手机银行登入版面



客户输入网上银行号码/用户名称、网上银行密码及验证码，然后按「登入」

企业网上银行

客户输入客户号码/客户别名、操作员编号及企业网上银行密码、验证码登入企业网上银行

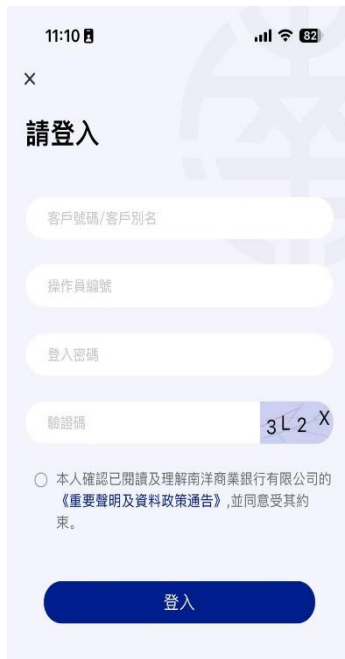


企业网上银行

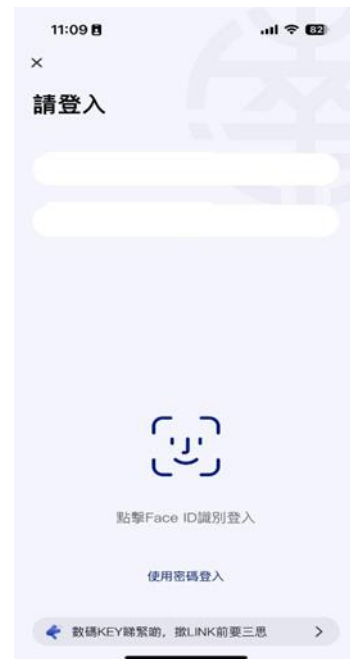
如客户已设置「双重认证登入」, 需在「保安编码器」输入企业网上银行生成的「挑战码」以获取由「保安编码器」发出的一次性「交易确认编码」以登入企业网上银行



企业手机银行



企业手机银行



5. 偽冒電郵、短訊及即時通訊訊息的常見特徵

- 請慎防「網絡釣魚」的騙徒訛稱本行之名發出虛假電郵、短訊及即時通訊訊息，企圖誘騙您提供帳戶資料、密碼、個人資料或信用卡號碼。下列為一些偽冒電郵、短訊及即時通訊訊息常見特徵，有助保持警惕。
- 內容出現語法不通、錯別字或拼寫錯誤。
- 內容通常涉及本行的重要訊息或要求提供個人資料以核實帳戶，例如：大額轉賬的交易通知或須啟用新的安全功能的通知，並要求點擊超鏈接或開啟附件。
- 電郵一般包含超鏈接或附件。屏幕顯示的超鏈接看似本行網址，但當用鼠標指向電郵顯示的鏈接時是其他網址。

6. 妥善保管個人密碼及個人資料

- 當收妥密碼函件後，應盡快透過網上服務更改密碼，然後將密碼函件銷毀。
- 請牢記密碼，切勿將密碼寫在或儲存在任何網上服務的裝置，或經常與此等裝置放在一起的對象上，亦切勿以任何形式記錄密碼而不加掩飾。
- 請定期更改密碼，切勿選用個人姓名、出生日期、身份證 / 護照號碼、電話號碼、幸運數字、及其他容易被猜中的個人資料、號碼或文字作為密碼或登入資料，並避免使用已於其他網站登記的密碼作為登入密碼。
- 切勿向任何人(包括本行職員及警方)透露網上銀行服務用戶名稱及密碼，亦不應隨便向任何人透露任何個人資料，如身份證/護照號碼、出生日期等。
- 切勿讓第三者使用您的網上銀行服務。
- 如遺失或外泄密碼或遺失保安設備，或懷疑密碼 / 保安設備遭盜用，或發現帳戶有未經授權的交易，請即與本行聯絡或直接聯絡香港警方。
- 請仔細核對月結單、通知書及確認書上的交易內容，如發現有錯漏或不正常交易，應即時通知本行。
- 您可透過網上銀行查詢您的帳戶交易紀錄和帳戶活動記錄，快捷方便。

7. 保護您的個人計算機

- 請定期下載並安裝操作系統及瀏覽器的更新程序。
- 請為個人計算機安裝防火牆。
- 請為個人計算機安裝病毒偵測軟件，並定期更新病毒定義文件及進行病毒掃描。
- 請設定難以猜破的鎖機密碼及使用自動上鎖功能。
- 切勿下載或安裝來歷不明的程序，亦不應開啟可疑的檔案或電子郵件，以防止黑客程序或計算機病毒盜取您的個人資料。
- 如透過無線網絡使用網上服務，客戶必須加強安全設定。

8. 使用網上銀行服務時須注意的安全措施

- 切勿在公共地方(如網上咖啡室或網吧)的公用計算機(或共用移動設備)使用網上銀行服務。
- 只設定及使用可靠的無線網絡上網。
- 切勿透過任何電子郵件、短訊或互聯網搜索器提供的超鏈接或二維條形碼登入網上服務。
- 登入網上服務前，請關閉其他瀏覽器窗口。此外，在使用網上銀行時，切勿同時開啟其他瀏覽器及瀏覽其他網站。
- 在登入網上服務時，請確定沒有其他人在旁窺視，以免泄露您的用戶名稱及密碼。

- 每次使用网上服务时，请先核对上一次登入及注销的纪录；客户亦应定期检查账户结余及核对交易纪录。如发现可疑情况，请即与本行联络。
- 当完成网上交易后，必须按「注销」离开系统，同时亦须关闭浏览器及删除浏览器的暂存及历史资料。
- 切勿在未注销网上银行服务前离开计算机。
- 有关其他使用互联网时应注意的保安措施，请参考常见问题。

9. 网上银行检视及调整各项服务限额

- 请定期检视您的各项服务的交易限额并作出适当调整（例如，降低转账限额）以符合您自身的安全保障需要。

手机银行安全资讯

提防流动装置恶意软件（Malware）骗案：

- 客户应只从官方认可的应用商店下载和安装由可信任开发商提供的已验证的应用程序，并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）。
- 在安装应用程序前，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。
- 切勿用 Jailbreak（越狱）或 Root 机等手法改装流动装置。
- 在任何情况都不应使用来历不明的应用程序。不要浏览可疑网站，或从这些网站下载任何档案。如发现任何可疑下载的程序，切勿尝试登入及停止操作，并建议即刻从手机中删除。
- 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 Android 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。

如何下载个人手机银行应用程序？

- 客户可于手机的浏览器键入 "www.ncb.com.hk/nanyang_bank/resource/pmbm/personalMobileBanking/index.html" 下载流动应用程序；
- 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」免费下载流动应用程序。
- 如发现任何可疑下载的程序，切勿尝试登入及停止操作。
- 谨防下载假冒流动应用程序，被植入钓鱼 / 木马程序盗取登入资料。
- 不要复制和安装不确定来源的手机银行客户端软件。
- 如发现任何不正常运作，例如出现异常版面或登入缓慢，请即停止操作。

手机银行的保安措施严密？

- 本行的网站采用了严密的 TLS 加密技术，透过个人化的登入名称及密码保障客户登入手机银行的安全。我们同时采用防止重复登入措施，即同一客户不能于不同手机或计算机同时登入。如客户使用服务时静止了一段指定时间，登入将被自动终止联机，防止任何未经授权的交易。

如何登入手机银行？

- 请透过官方软件应用商店下载"NCB (南商)"流动应用程序，开启应用程序并按“登入”后，以相关网上银行号码/用户名称及密码登入手机银行。

手机银行有否获得任何安全认证？

- 本行的手机银行获 Sectigo 颁予安全认证。

使用手机银行时应特别注意的事项？

- 切勿在浏览器选择储存或保留密码，并关闭浏览器的「自动完成」设定，防止第三者从浏览器盗取您的登入资料。
- 避免使用公众地方或缺密码保护的无线网络(即 Wi-Fi)登入手机银行，建议使用已加密及可靠的网络连接互联网以登入手机银行。
- 为流动装置设定自动锁定功能及避免于环境挤迫的地方登入手机银行，并留意在个别流动装置输入密码时，有关密码可能以明码的方式放大，间接让第三者窥视登入资料。
- 关闭无需使用的无线网络功能(如 Wi-Fi、蓝牙、NFC)或支付应用程序。如需使用 Wi-Fi，应选用加密的网络，并关闭 Wi-Fi 自动联机设定。
- 避免使用他人的流动装置登入手机银行及让他人使用您的流动装置。
- 建议在流动装置安装防火墙及防病毒软件/手机保安应用程序，并定期更新。请参考香港计算机保安事故协调中心网页：<https://www.hkcert.org/mobile-security-tools>，选择合适的应用程序。
- 为确保您的网上交易安全稳妥，使用本行流动应用程序时，本行会检查流动装置是否使用已被破解及符合基本保安要求的操作系统，客户或将不能透过相关的流动装置使用手机银行，请注意相关提示讯息。
- 每次使用手机银行时，请先核对上一次登入及注销的纪录；您亦应定期检查账户结余及核对交易纪录。本行为客户提供手机银行（个人及企业）的登入记录；客户可登入手机银行后查阅近期登入记录（个人手机银行：查看更多设置 > 安全 > 登入日志；或企业手机银行：我的），包括登入时间、位置信息、和设备信息，以便及时发现潜在异常活动。
- 如发现可疑情况，请即与本行联络。
- 客户须妥善保管个人密码及个人资料并对此负责：
 - 请牢记密码，切勿将密码写在任何已安装手机银行的装置，或经常与此等装置放在一起的对象上，亦切勿把密码储存在手机内或以任何形式记录密码而不加掩饰。
 - 切勿选用您的个人姓名、出生日期、身份证 / 护照号码、电话号码、幸运数字、及其他容易被猜中的个人资料、号码或文字作为密码或登入资料，并避免使用于其他网站登记的密码作为登入密码。
 - 切勿向任何人(包括银行职员及警方)透露您的手机银行用户名称及密码，亦不应随便向任何人透露您的个人资料，如身份证 / 护照号码、出生日期等。
 - 切勿让第三者使用您的手机银行或密码。
 - 请定期更改密码。
 - 如遗失或外泄密码或遗失保安设备，或怀疑密码 / 保安设备遭盗用，或发现账户有未经授权的交易，请即与本行联络或直接联络香港警方。
- 请定期透过官方软件应用商店(如 Google Play，App Store 及华为香港应用市场等)或本行网站下载并安装本行流动应用程序、其他应用程序、手机操作系统及浏览器的最新版本。切勿尝试安装来源不明的软件/应用程序。如发现任何可疑的程序，切勿尝试下载、登入及应实时停止操作。
- 切勿随意透过任何社交平台获取不知明的二维码以进行付款交易，请确保来源可靠。

- 当扫描二维码时，请提高警觉并确保二维码的来源可靠。
- 在扫描二维码或经识别代号付款前，应仔细核对收款人屏蔽名称的提示。
- 在扫描二维码付款前，应仔细核对商店或商户之名称。
- 请仔细核对由二维码产生之交易资料是否正确。
- 完成交易后，请核对银行所发出之交易纪录。
- 除非您进行转账或支付服务等交易，切勿随意向他人展示由本银行应用程序所生成的二维码。
- 您须采取一切合理的审慎措施，稳妥保管您的流动装置。假如您发觉您的流动装置遗失或被盗用，或曾发生任何未经授权交易，请即与本银行联络或直接联络香港警方。

使用生物认证服务时应特别注意的事项？

- 当您成功登记「生物认证」服务后，任何储存于您的流动装置之指纹或 Face ID 均能使用「生物认证」服务。您必须确保只有您的指纹或 Face ID 储存于您的流动装置，并确保流动装置上用作储存指纹或 Face ID 及登录「生物认证」服务的保安密码或编码保密。
- 基于保安理由，切勿使用已被破解的流动装置。
- 如要取消「生物认证」服务，您可以透过登入手机银行，进入「流动保安编码」关闭生物认证设定选项。请注意于取消「流动保安编码」服务后，您的指纹或 Face ID 仍储存于您的流动装置上，您可考虑因应情况自行决定删除有关资料。
- 如您的流动装置的指纹或 Face ID 记录曾经变更，您的「生物认证」服务会被暂停，您需要重新登记或启用「生物认证」服务。
- 如您有理由相信您的生物认证资料可能与其他人相同或非常相似，切勿使用生物认证资料作生物认证。例如您有双胞胎或三胞胎兄弟姊妹的话，切勿使用面孔辨识功能作认证。
- 如您的生物认证资料正在或将会经历迅速发展或改变，切勿使用有关生物认证资料作生物认证。例如您正值青少年时期，面部特征正迅速发育，切勿使用面孔辨识功能作认证。

若我在交易中途，有电话来电或忽然失去了网络讯号，如何确认已成功递交交易指示？

- 如指示已成功递送及执行，手机银行的版面会显示有关交易的参考编号。您亦可查看最近十笔交易纪录，以确认指示是否已成功递送及执行。

注销手机银行后，是否需要关闭浏览器？

- 本行建议您注销系统后同时关闭浏览器。此外，您亦须定时删除浏览器的暂存及历史资料。

南商 e+流动应用程序安全资讯

如何下载南商 e+流动应用程序(「南商 e+」)？

- 客户请透过官方软件应用商店 (如 Google Play，App Store 及华为香港应用市场等) 搜寻「南商 e+」免费下载流动应用程序。
- 如发现任何可疑下载的程序，切勿尝试登入及停止操作。
- 谨防下载假冒流动应用程序，被植入钓鱼 / 木马程序盗取登入资料。
- 不要复制和安装不确定来源的应用程序客户端软件。
- 如发现任何不正常运作，例如出现异常版面或登入缓慢，请即停止操作。

南商 e+的保安措施？

- 南商 e+采用了严密的 128 位加密技术，透过本人的手机号码及短信一次性密码保障用户登入南商 e+的安全。如用户使用服务时静止了一段指定时间，登入将被自动终止联机，防止任何未经授权的行为。

如何登入南商 e+？

- 请透过官方软件应用商店下载南商 e+，开启应用程序，需输入用户本人的手机号码和短讯一次性密码登入南商 e+。
- 用户在登入南商 e+ 查看账户信息或更新开户申请资料时，除需要输入本人手机号码、短讯一次性密码外，还需同时输入「南商 e+登录密码」。

使用南商 e+时应特别注意的事项？

- 避免使用公众地方或缺密码保护的不安全无线网络(即「Wi-Fi」)使用本流动应用程序。使用流动应用程序建议使用已设定及可靠的网络连接互联网。
- 为流动装置设定自动锁定功能及避免于环境挤迫的地方登入南商 e+，并留意在个别流动装置输入密码时，有关密码可能以明码的方式放大，间接让第三者窥视登入资料。
- 关闭无需使用的无线网络功能(如 Wi-Fi、蓝牙、NFC)。如需使用 Wi-Fi，应选用加密的网络，并移除不必要的 Wi-Fi 联机设定。
- 避免使用他人的流动装置登入南商 e+及让他人使用您的流动装置。
- 用户应避免连接流动装置至任何怀疑被计算机病毒感染的个人计算机，以防流动装置亦被感染，同时，建议在流动装置安装防火墙软件及防手机病毒软件。不应使用已被破解的 iPhone 或 Android 手机流动装置尝试使用流动应用程序，以防潜在保安漏洞，并可在软件应用商店下载合适的流动保安应用程序，您可参考香港计算机保安事故协调中心网页：<https://www.hkcert.org/mobile-security-tools>，选择合适应用程序。
- 为确保您的个人资料安全稳妥，使用本流动应用程序时，本行会检查装置是否使用已被破解及符合基本保安要求的操作系统，客户或将不能透过相关的装置使用本流动应用程序，请注意相关提示讯息。
- 用户需为流动装置设定自动锁定功能，及切勿选用容易被猜中的个人资料、号码或文字作为密码，并避免使用于其他网站登记的密码作为登入密码。请定期透过指定官方软件应用商店(详情请参阅本行网站)或本行网站下载并安装本流动应用程序及其他应用程序、手机操作系统及浏览器的更新程序。
- 下载或使用南商 e+时，本行会记录您的移动设备信息(包括 IP 地址、设备 ID 和操作系统)、登录和注销时间，以用于操作优化、统计分析和反欺诈。相关信息的保留时间不会超过实现目的所需的时间。
- 用户须妥善保管南商 e+登录密码及个人资料并对此负责：
 - 请牢记南商 e+登录密码，切勿将密码写在任何南商 e+的装置，或经常与此等装置放在一起的对象上，亦切勿把密码储存在手机内或以任何形式记录密码而不加掩饰。
 - 切勿选用您的个人姓名、出生日期、身份证 / 护照号码、电话号码、幸运数字、及其他容易被猜中的个人资料、号码或文字作为南商 e+登录密码，并避免使用于其他网站登记的密码作为登入密码。
 - 切勿向任何人(包括银行职员及警方)透露您的登录密码，亦不应随便向任何人透露您的个人资料，如身份证 / 护照号码、出生日期等。
 - 切勿让第三者使用您的南商 e+流动应用程序或登录密码。
 - 请定期更改登录密码。
 - 如遗失或外泄密码或遗失保安设备，或怀疑密码 / 保安设备遭盗用，或发现账户有未经授权的交易，请即与本行联络或直接联络香港警方。
- 您须采取一切合理的审慎措施，稳妥保管您的流动装置。假如您发觉您的流动装置遗失或被盗用，或曾发生任何未经授权交易，请即与本行联络或直接联络香港警方。

若我在南商 e+ 上提交开户申请时中途退出，是否还能继续原有的申请流程？

- 如您还未提交申请，南商 e+ 和微信官号手机开户申请页面均不保留申请过程中填写的信息或上传的文件。

若我忘记安全问题答案及南商 e+ 登录密码，要如何重设密码？

- 如您还没有提交银行开户申请，可以通过短讯一次性密码验证身份来重设登录密码和安全问题；
- 如您已递交开户申请但尚未开立银行账户，只能通过短信一次性密码验证身份后，通过取消开户申请来重设密码和安全问题；
- 如您已提交申请且银行账户已开立，将无法重设密码，只能通过在线聊天室联系客服或亲临分行查看银行账户信息。

微信官号安全资讯

搜寻本行微信官方账号时，请参照本行注册的 WeChat ID - NCB_HK，以确保微信官号的服务及资讯由本行提供，切勿于未经认证的微信账号透露任何个人及账户资料，如有疑问，请与本行职员联络。

使用微信官号时应注意的事项：

- 进行绑定时，用户需使用个人网上银行账户、密码及于本行登记的手机号码收取的「短讯一次性密码」进行验证。
- 切勿透过任何电子邮件或短讯提供的超链接或二维码登入微信官号。
- 切勿在微信对话框输入个人敏感资料，本行不会以微信对话框要求用户提供其账户号码、私人密码或任何个人资料。
- 如欲了解更多绑定时需注意的事项，可于微信对话框输入「绑定服务指南」关键词查询。
- 如有查询、报告保安问题或要求取消绑定，请致电：+852 2616 6628
- 为确保客户资料安全，建议操作系统及浏览器如下：
 - iOS 9.0 或以上(预设浏览器)，WeChat 8.0.45 或以上
 - Android 4.4 或以上(预设浏览器)，WeChat 8.0.45 或以上
- 请定期下载并安装流动应用程序、操作系统及浏览器的更新程序。

自动柜员机及提款卡的安全资讯

保护个人密码及提款卡

- 若您选择银行预设密码，请在收妥提款卡及密码后，谨记您的个人密码并将密码通知书销毁。
- 请在收妥提款卡及密码通知书后，再通过网上银行、手机银行、24 小时提款卡服务热线 (852)26166266，或至我行任一分行办理提款卡激活手续。
- 请在激活提款卡后，尽快通过自动柜员机或分行办理更改密码。
- 请您采取合理步骤妥善存放卡，并将认证因素保密以防止欺诈行为。
- 请小心保管您的提款卡，应毁灭印有个人密码的通知书并牢记您的个人密码及定期更改密码。
- 请勿直接将密码抄下或记录，而不加掩藏。无论在任何情况下，请避免在提款卡上或任何其他经常与提款卡放在一起的对象上，写上个人密码。
- 基于安全理由，您应避免使用身份证号码、出生日期、电话号码、常见数字组合(如 123456)或其他容易被猜中的数字组合作为密码。同时避免以相同密码来操作其他服务，包括登入网上银行或其他网址。
- 不应让任何其他人士使用您的提款卡或认证因素。
- 请您在发现卡有异常或可疑交易后，应尽快通知本行。

- 警方及銀行職員不會要求您透露個人密碼；在任何情況下，切勿向他人透露個人密碼。
- 用自動櫃員機前請留意鍵盤保護罩有否異樣(如被移除或加裝鏡頭)及插卡口和鍵盤有否可疑裝置。如發現可疑裝置，應立即通知有關銀行。
- 當您在自動櫃員機或消費終端機輸入個人密碼時請以手遮蓋鍵盤，請確保您的個人密碼及賬戶資料不會被第三者看見。
- 本行或因應情況向您發放保安提示手機短訊或通訊，如收到後請即時查閱。
- 如您發現或懷疑您的提款卡及/或認證因素遺失、被盜用、外泄或遭未經授权使用，應即致電 24 小時提款卡服務熱線 (852) 2616 6266。
- 在您通知本行您的提款卡/認證因素遺失、被盜取或認證因素或提款卡的数据已經泄露前，您可能承擔因您的提款卡被用作未經授權交易而產生的有關損失。如您未作出任何欺詐或嚴重疏忽行為，並在發現您的提款卡/認證因素遺失或被盜取，或認證因素或提款卡数据已遭泄露後，在可能情況下儘快通知本行，您就此類提款卡損失要承擔的責任以本行指明的限額為限，但不應超過 500 港元。此限額僅適用於有關卡賬戶關聯的損失。

小心處理提款

- 當您提款時請避免分心而忘記提取鈔票及提款卡，並應即時點算鈔票數目及保留任何單據。
- 請勿取去他人遺留於自動櫃員機出錢槽的鈔票或插卡口的提款卡，應待鈔票或提款卡自動退回機內。

防范提款卡騙案

- 提款卡騙案包括盜取提款卡或相關資料：姓名、卡號、有效日期及驗證碼/ CVV 碼。騙徒通常會透過惡意軟件、偽冒電郵、釣魚網站，甚至從垃圾箱中的提款卡相關信件獲取提款卡的詳細資料。您在棄置提款卡相關信件前，應先將其撕碎損毀。假如您發覺您的提款卡被盜或曾發生任何未經授權交易，請即與本行聯絡或直接聯絡香港警方。

安全使用境外自動櫃員機

- 您可憑提款卡於境外《銀聯》網絡自動櫃員機提款，每筆提款交易手續費為港幣/人民幣 50 元。如需了解目的地的自動櫃員機位置及能否支持境外提款，可瀏覽《銀聯》網頁：www.unionpayintl.com/hk/
- 為加強保安，所有提款卡於境外自動櫃員機之提款限額預設為港幣 0 元。如需要在境外提款，請預先在離港前透過網上銀行、手機銀行、銀通網絡自動櫃員或 24 小時提款卡服務熱線 (852) 2616 6266 設置有關提款限額及有效限期。詳情請瀏覽“加強香港境外自動櫃員機服務保安措施的通知”：www.ncb.com.hk/nanyang_bank/popup1/ncb_esm_chi.html

安全使用境外刷卡消費服務

- 除可憑卡透過「易辦事」消費，您亦可在香港、中國內地及海外，于接受「銀聯」的商戶刷卡付款。若有需要，您可通過分行、24小時提款卡服務熱線(852)2616 6266申請關閉境外消費服務。

自动柜员机的正常入卡位



存支票机的正常入卡位



被装置读卡器的入卡位



存钞机的正常入卡位



双重认证工具

为提升网上保安，本行网上及手机银行为客户提供「保安编码器」及「流动保安编码」作为双重认证工具。为了方便视障人士使用网上银行/手机银行，本行还提供具有语音功能的“安全密码器”。客户必须使用「保安编码器」或「流动保安编码」及同意以指定方式接收交易通知，方可于网上及手机进行「指定交易」。有关网上及手机使用双重认证办理指定交易详情，请浏览本行网页：「电子银行服务 > 双重认证」。

此外，企业客户可于任何一家分行申请「保安编码器」作为双重认证工具。

流动保安编码

「流动保安编码」为您带来安心及便捷的理财体验，南商流动应用程序内置「流动保安编码」功能，启用后便无须携带实物「保安编码器」。

当您于指定型号流动装置完成后启用程序后，便可实时透过自定义密码或「生物认证」开启「流动保安编码」，以确认手机银行指定交易。此外，您亦可使用「流动保安编码」产生的一次性「保安编码」/「交易确认编码」，确认个人网上银行指定交易。

「流动保安编码」的注意事项：

- 基于保安理由，客户只可于一部流动装置上启用「流动保安编码」。并请勿在他人的手机上登入手机银行及启用「流动保安编码」。
- 个人客户于成功后启用「流动保安编码」后，所持有的「保安编码器」(如有)将会自动被停用。如客户重新使用「保安编码器」，需要先于流动装置上停用「流动保安编码」，并前往本行各分行重启「保安编码器」，企业客户可透过企业网上银行重启。
- 请妥善保管已启用「流动保安编码」的流动装置，如发现或怀疑已启用「流动保安编码」的流动装置遗失或被窃，可以透过另一流动装置停用流动保安编码。

「生物认证」

如您启用「流动保安编码」，您可同时于指定型号的流动装置上登记使用于流动装置上的「生物认证」(例如：指纹、Face ID)以：

- 登入手机银行
- 开启「流动保安编码」以确认手机银行指定交易
- 开启「流动保安编码」以获取一次性「保安编码」/「交易确认编码」以确认个人网上银行指定交易

如需了解如何启用「流动保安编码」、操作系统要求及兼容流动装置，请浏览：

www.ncb.com.hk/nanyang_bank/faq/person-bank/SecurityCode

请您妥善保管您的生物认证资料，包括且不限于指纹、面貌特征或其他由本行不时认可的生物特征等，并确保指定流动装置上用作储存生物认证资料及登记生物认证的保安密码或编码保密。如您怀疑或发觉您的生物认证资料被盗用，请即与本行联络或直接联络香港警方。

保安编码器

客户可透过本行网上银行、任何一间分行申请「保安编码器」。收到客户申请后，我们会将「保安编码器」邮寄至客户登记的通讯地址。

当您使用「保安编码器」时，请注意以下事项：

- 客户必须于本行登记手机号码及启动双重认证功能后，方可申请「保安编码器」。客户可亲临本行任何一家分行办理。
- 当客户收到「保安编码器」后，请即登入网上银行，并按指示启用「保安编码器」。
- 客户不用安装额外软件/驱动程序，亦不需依赖第三方单位传输授权码，安全可靠。
- 企业客户如设置了双重认证登入，需在「保安编码器」输入企业网上银行生成的「挑战码」以获取由「保安编码器」发出的一次性「交易确认编码」以登入企业网上银行。
- 客户于进行「指定交易」时，需于「保安编码器」上输入是次交易的资料(「挑战码」)，从而产生一次性「交易确认编码」。



- 请妥善保管「保安编码器」，切勿将「保安编码器」交予第三者使用或随意摆放。如有遗失或损毁，请立即与本行职员联络。

「保安编码器」是怎样运作的？

- 每个「保安编码器」具有独立的机身编号，并内置资料及时钟。在您启用「保安编码器」后，内置的时钟将与本行系统同步。当您按下「保安编码器」的按钮后，「保安编码器」即会根据资料及内置时钟，产生一次性的「保安编码」。此编码只于短时间内有效，并只供系统核实客户身份之用。如您未能于时限内输入「保安编码」，则需要重新按钮以获取新的「保安编码」。

如何使用「保安编码器」？

- 因应不同的交易类别，客户可使用「保安编码器」获取不同的「保安编码」，并根据网上指示进行验证
 - 客户在登入企业网上银行或进行「一般交易」时，只需按「保安编码器」右下方的按钮，液晶显示屏即会显示一组六位数字所组成的「保安编码」。「保安编码」只可使用一次，并于短时间内有效。
 - 客户进行「指定交易」时，请按「保安编码器」左下方的按钮，然后使用数字键输入网上以红色标示的数字资料。输入所需资料后，请按「保安编码器」左下角的按钮，液晶显示屏即会显示一组由六位数字所组成的「交易确认编码」。「交易确认编码」只可使用一次，并于短时间内有效。

于网上银行输入「保安编码」或「交易确认编码」后，为什么仍不能核实我的交易指示？

- 网上银行未能核实您的交易指示，可能是以下原因所致：
 - 客户输入了错误编码
 - 客户输入编码时已超过了编码的有效时间
 - 「保安编码器」受到撞击或曾受过热、过冷、潮湿或磁场等环境影响
- 请根据网上指示重新输入一个有效的「保安编码」或「交易确认编码」。如仍未能核实交易指示，请与本行职员联络，以重设编码器状态。
- 若在重设编码器状态后，仍未能完成核实程序，客户可免费更换一个新的「保安编码器」。

如果「保安编码器」的液晶体屏幕显示「BATT」讯息，我应该怎么办？

- 「BATT」意指「保安编码器」的电池将耗完。该电池一般可使用3至5年，惟视乎使用情况而定。如个人客户须更换「保安编码器」，请亲临本行任何一家分行办理。请注意，「保安编码器」的电池不能更换，任意改动「保安编码器」的内部零件将导致设备失灵。

启用「保安编码器」的「一次性密码」及「完成指定交易通知」手机短讯

- 启用「保安编码器」的「一次性密码」及「完成指定交易通知」手机短讯(如有)只会传送至您于本行登记的手机号码。即使您已启动以下的本地手机服务供货商提供的「短讯转驳服务」，上述短讯亦不会被转送至其他手机号码：
 - 数码通电讯有限公司
 - 香港移动通讯有限公司
 - 和记电话有限公司
 - 中国移动香港有限公司
- 请仔细核对本行透过手机短讯及电邮发出的交易资料是否与您在网上/手机银行上办理的交易相符，如有任何疑问，请实时与本行联络。

常见问题

甚么是 TLS(“Transport Layer Security”)加密技术？

- 网上银行所采用的 TLS 加密技术(TLS v1.2 及以上), 为现时在商界广泛应用的网上保安标准。所有透过网上服务传送的资料均会以此技术进行加密处理, 以保障客户资料的安全。

当我设定密码或登入资料时需注意甚么？

- 不应使用出生日期、身份证/护照号码、电话号码或英文姓名作密码或登入资料。
- 不应使用连续三个或以上的相同英文字母或数字, 例如「333」、「bbb」等。
- 不应使用顺序的英文字母或数字, 例如「123」、「abc」等。
- 不应使用与用户名称相同的密码。
- 不要以相同的密码接驳其他服务(如接连互联网或其他网址)。

我需要在甚么时候更改密码？

- 您应定期更改密码。如客户于一段时间内未有更改密码, 本行系统将自动提示客户更改。

我应如何保护个人资料？

- 当您使用网上服务时, 可能需输入个人资料(如身份证/护照号码、出生日期等)作为额外身份核证, 但您应保持警惕, 不要随便向任何人透露上述个人资料, 并应妥善处理载有个人资料的文件(如个人信件及月结单等)。

为何需要更新操作系统及浏览器？

- 定期检查及下载软件供货商提供的「增补程序」, 有助修正操作系统或浏览器的保安问题, 避免您的计算机受到病毒或黑客入侵及盗取资料。

我应如何设定无线网络的保安措施？

- 无线网络存取点(Access Point 或「AP」)应避免太接近门窗, 以减低被第三者截收并破解无线网络内容的风险。
- 开启保护无线网络的设定, 切勿向任何人透露您的无线网络保安设定。

使用互联网需注意甚么保安措施？

- 如使用电子工具储存个人资料, 请将资料加密, 以防止第三者盗取及使用。
- 切勿在浏览器选择储存或保留密码, 并关闭浏览器的「自动完成」设定, 防止第三者从浏览器盗取您的资料。
- 关闭窗口系统的「档案及打印分享」功能, 并限制计算机用户的访问权限, 以免第三者透过网络盗取您的个人资料。
- 切勿下载或安装非法或来历不明的软件, 以免感染计算机病毒或木马程序。在开启任何外来档案前, 先以防毒软件进行扫描。

我可以从哪里获得更多关于使用网上银行及自动柜员机服务的保安资讯？

- 香港金融管理局 – 智醒消费者 小心骗徒!
https://www.hkma.gov.hk/gb_chi/smart-consumers/beware-of-fraudsters/
- 香港金融管理局 – 智醒消费者 网上银行
<https://www.hkma.gov.hk/chi/smart-consumers/internet-banking/#using-internet-banking-services>
- 香港金融管理局 – 智醒消费者 自动柜员机
<https://www.hkma.gov.hk/chi/smart-consumers/atms/>
- 香港银行公会 - 参考资讯「智醒消费者 安全小贴士」
<https://www.hkab.org.hk/tc/useful-information/smart-consumer#security-tips>
- 香港警务处有关网络安全及科技罪案
https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/
- 政府资讯科技总监办公室 – 「资讯安全网」
<https://www.infosec.gov.hk/tc/>
- 香港银行公会 – 「提升保安措施 助客户免受恶意程式诈骗」
<https://www.hkab.org.hk/tc/news/press-release/292>

本行热线及网址

- 客户服务热线 (852) 2616 6628
- 24 小时提款卡服务热线 (852) 2616 6266
- 24 小时电子银行保安热线 (852) 2616 6628
- 网址 www.ncb.com.hk
- 个人网上银行 <https://pnb.ncb.com.hk/#/login>
- 企业网上银行 <https://cpb.ncb.com.hk/#/login>