NCB 南洋商業銀行

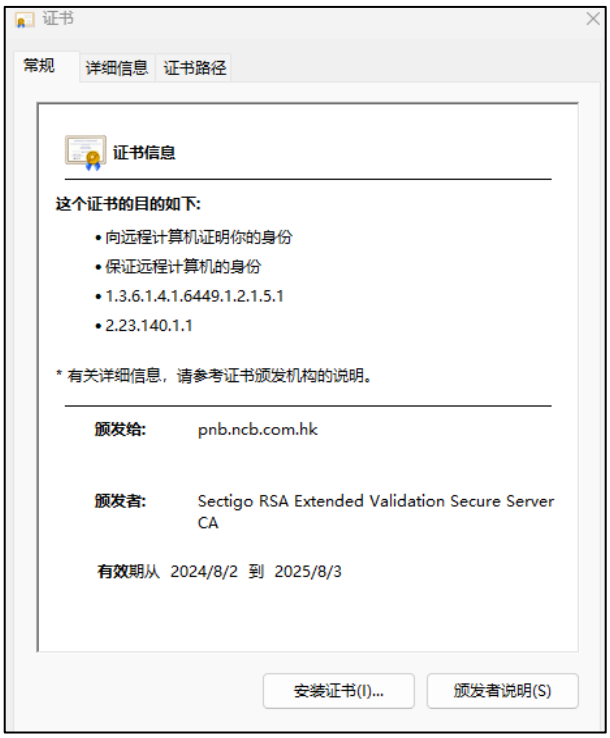
网上保安提示及资讯

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。
- 本行网上银行及手机银行设有多种网络安全保护方案，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，支持客户查阅登入记录，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。详情请参阅「双重认证工具」
- 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

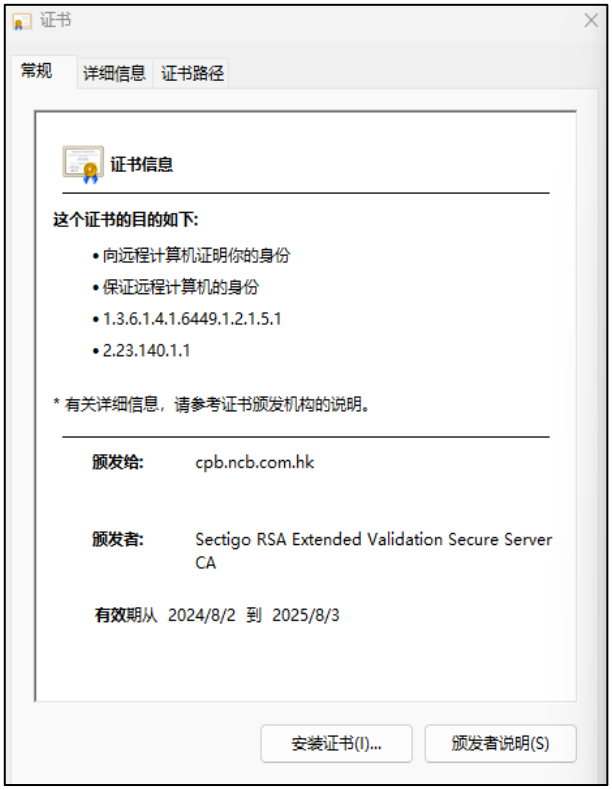
- 本行采用扩展验证 SSL 证书，让客户可透过检视浏览器的地址栏，核定所进入的网页是否本行的真确网页。
- Microsoft Internet Explorer 版本 9 或以上浏览器的地址栏为绿色，是扩展验证 SSL 的其中一个保安特征。如客户选用 Microsoft Internet Explorer，亦可在网上银行的登入版面上按「安全锁」标志，以查阅证书内容，包括其有效日期及以下资料。请注意，各项资料的显示方式会因不同浏览器版本而有所差异。有关扩展验证 SSL 证书详情，请浏览证书发行者 Sectigo 的网页。



个人网上银行

发给：pnb.ncb.com.hk

发行者：Sectigo RSA Extended Validation Server CA



企业网上银行

发给：cpb.ncb.com.hk

发行者：Sectigo RSA Extended Validation Server CA

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**
  - 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）
- **企业网上银行**
  - 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）

网上保安提示

防范伪造网站

- 请保持警觉并注意任何试图冒充本行网址或网上银行服务的伪造网站。客户必须完全确定浏览或登入本行官方网站或网上银行服务，否则不应提供任何相关的网上服务资料。

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。

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。

浏览器中间人攻击

- 曾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。

请参阅以下网上银行/手机银行登入版面

- **个人网上银行登录**

持有「保安编码器」或「流动保安编码器」客户必须以「双重认证」方式登入，输入网上银行号码/用户名称、网上银行密码及验证码后，点击「登入」，客户需进一步输入由「保安编码器」或装置上的「流动保安编码器」发出的一次性「保安编码」以登入个人网上银行。

- **个人手机银行登录**

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」。

或者以「生物认证」进入个人手机银行。

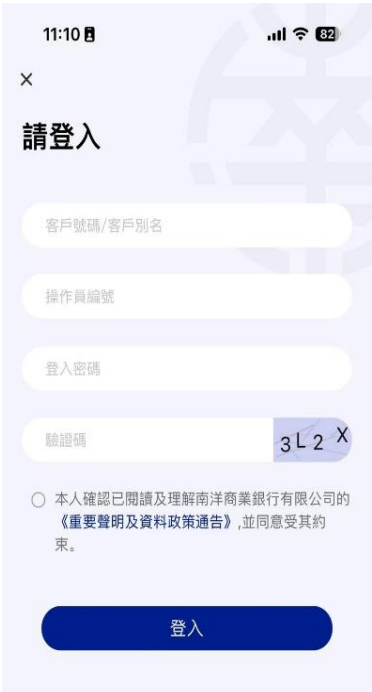
- **企业网上银行登录**

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。

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。

- **企业手机银行登录**

客户输入网上银行号码/用户名称、操作员工编号及网上银行密码及验证码，然后按「登入」。



或者以「生物认证」进入企业手机银行。

伪冒电邮、短讯及实时通讯讯息的常见特征

- 请慎防「网络钓鱼」的骗徒讹称本 行 之名发出虚假电邮、短讯及实时通讯讯息，企图以各种方式诱骗您提供账户资料、密码、个人资料或信用卡号码。
- 「网络钓鱼」的骗徒发出虚假电邮、短讯及即时通讯讯息内容出现语法不通、错别字或拼写错误。通常涉及本行的重要讯息或要求提供个人资料以核实账户，例如：大额转账的交易通知或须启用新的安全功能的通知，并要求点击超链接或开启附件。
- 电邮一般包含超链接或附件。屏幕显示的超链接看似本行网址，但当用鼠标指向电邮显示的链接时是其他网址。

妥善保管个人密码及个人资料

- 请牢记密码，切勿将密码写在或储存在任何网上服务的装置，或经常与此等装置放在一起的对象上，亦切勿以任何形式记录密码而不加掩饰。

- 请定期更改密码，切勿选用个人姓名、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，并避免使用已于其他网站登记的密码作为登入密码。
- 切勿向任何人(包括本行职员及警方)透露网上银行服务用户名称及密码，亦不应随便向任何人透露任何个人资料，如身份证/护照号码、出生日期等。
- 切勿让第三者使用您的网上银行服务。
- 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。
- 请仔细核对月结单、通知书及确认书上的交易内容，如发现有错漏或不正常交易，应实时通知本行。
- 您可透过网上银行查询您的账户交易纪录和账户活动记录，快捷方便。

保护您的个人计算机

- 请定期下载并安装操作系统及浏览器的更新程序。
- 请为个人计算机安装防火墙。
- 请为个人计算机安装病毒侦测软件，并定期更新病毒定义文件及进行病毒扫描。
- 请设定难以猜破的锁机密码及使用自动上锁功能。
- 切勿下载或安装来历不明的程序，亦不应开启可疑的档案或电子邮件，以防止黑客程序或计算机病毒盗取您的个人资料。
- 如透过无线网络使用网上服务，客户必须加强安全设定。

使用网上银行服务时须注意的安全措施

- 切勿在公共地方(如网上咖啡室或网吧)的公用计算机（或共用移动设备）使用网上银行服务。
- 只设定及使用可靠的无线网络上网。
- 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或二维条形码登入网上服务。
- 登入网上服务前，请关闭其他浏览器窗口。此外，在使用网上银行时，切勿同时开启其他浏览器及浏览其他网站。
- 在登入网上服务时，请确定没有其他人在旁窥视，以免泄露您的用户名称及密码。

- 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。
- 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。