

手机银行安全资讯

关于留意流动装置恶意软件（Malware）骗案资讯，请见“最新/重要保安资讯”。

下载个人手机银行应用程序注意事项

- 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。

- 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，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，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。

使用手机银行进行交易注意事项

- 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关闭设定。请注意于取消「生物认证」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。