

# 南商保安提示

升级保安措施 | 防骗小贴士



## 升级保安措施您要知 「网银安全 ABC」

### A - App 内认证 (Authenticate in-App)

当您首次登入或更换以其他未经绑定的流动装置登入手机银行时，  
须透过人脸识别等双重认证方式进行验证，以完成安全设置：

- 启用安全设备绑定
- 启用流动保安编码器



当您登入网上银行或进行指定交易\*时，须透过流动保安编码器/保安编码器等  
双重认证方式进行验证，不再使用一次性短讯密码。

\*指定交易包括但不限于：

- 重设登入密码
- 投资服务
- 转账至未登记收款人
- 登记收款人
- 调高交易限额
- 登记小额转账
- 银通无卡提款
- 更新客户资料
- 南商微信官方账号账户绑定服务



## B - Bye Bye 高危功能 (Bye to unused functions)

您可随时透过手机银行/网上银行，选择停用以下两项  
风险较高的服务



- 网上新增登记第三者收款人服务
- 网上提升转账/汇款限额服务

## C - Cancel 可疑转账 (Cancel suspicious payments)

当您向可疑账号发起转账交易时，「可疑账号警示」将会  
弹出并显示一段时间，让您有充足时间查阅警示内容。



### 防骗小贴士

#### 警惕诈骗来电、手机短讯、电邮

- 请保持警觉并慎防伪装本行的欺诈电话、网站、电邮、短讯、手机应用程序及社交平台账号。请不要单凭来电显示、电邮地址、网址、短讯或讯息内容辨别来电者/发送人的身份。
- 本行不会透过电话、电话录音、电邮或短讯等方式向您收集任何个人敏感资料(包括网上/手机银行服务的用户名称、登入密码、一次性密码、保安编码及交易确认编码)，亦不会透过预录语音信息通知客户银行户口出现异常。
- 如有怀疑，请致电本行 24 小时保安热线 (852) 2616 6628 (选择语言后按“9”)核实有关信息内容、来电者及讯息发送人的身份，或可致电香港警务处反诈骗协调中心的 24 小时咨询热线 18222 以寻求警方协助。

## 慎防网络钓鱼

- 请避免使用公众地方或欠缺密码保护的无线网络(即 Wi-Fi)登入网上银行。
- 您不应透过第三者网站/手机应用程序、电邮、短讯或实时通讯讯息中的超链接、二维码或附件登入本行的网上/手机银行, 或提供个人或银行账户等资料。
- 请透过官方应用商店(如 Google Play, App Store 及华为香港应用市场等)下载本行手机银行应用程序和南商 e+流动应用程序, 切勿尝试下载或安装任何来历不明或可疑的软件/应用程序。如发现任何可疑的程序, 切勿尝试登入或使用, 并应立即停止操作。
- 您必须完全确定登入本行官方网站, 否则不应提供任何网上银行相关的资料。如有疑问, 请与本行职员联络。
- 请注意登入时有否异样(例如: 出现可疑的弹出窗口、窗口运作缓慢、重复要求输入密码等)。如有怀疑, 切勿按照可疑页面上的指示操作或输入任何数据, 并应立即关闭浏览器及与本行联络。

## 网上交易安全提示

- 请定期查阅您的户口交易纪录及本行发出的交易通知,如发现任何怀疑未经授权的交易,请立即通知本行。
- 如果发现网上银行账户出现异常或可疑交易/活动,您可以拨打本行 24 小时保安热线 (852) 2616 6628 要求实时暂停网上银行服务。
- 请定期检视您的交易限额设定并作出适当调整(如降低转账限额),以符合您自身的安全保障需要。
- 当输入认证因素以进行网上交易认证时,请小心核对交易详情,例如:交易类别、交易金额及货币等。如有查询,请立即与本行联络。

## 认证因素安全提示

- 请定期更改并使用保安程度较高的登入密码，避免使用相同的密码接驳其他服务。
- 请不要向任何人(包括本行职员、警方、来电者)提供任何个人敏感资料(包括网上/手机银行服务用户名称、登入密码、一次性密码、保安编码及交易确认编码)。
- 如您曾向第三者透露登入密码，请立即与本行联络并更改密码。
- 请妥善保管您的认证因素(如登入密码及认证令牌)，切勿将密码储存或写在任何装置。
- 为保护您的提款卡密码，使用自助银行服务输入密码时，请用手遮掩键盘，若发现有不明装置，请勿使用。
- 如遗失或外泄密码/认证因素，或怀疑密码/认证因素遭盗用，或发现账户有未经授权的交易，请即与本行联络。

想了解更多？

请参阅本行官网>保安资讯