华南商业银行
网上银行安全小秘诀手册

只要掌握「网上银行」操作安全小秘诀，您就可安心享受具备最高安全且操作便利的『华南银行网上银行』卓越的理财服务。

~~目录~~

◎ 如何自我保护

1. 设定网上银行密码时提高警觉

ANS：

① 为了不让有心人士轻易猜中您的密码，提醒您不要使用公民身份号码（身分证字号）、生日、电话号码或具规则性排列等容易被猜中的英文字元串或数字作为密码，并应妥善保管及不定期的「变更密码」也是保管密码的好方法。

② 切勿使用您在其它网络服务的账户名称及密码，例如电子邮件或网络简讯，以免被有心人士猜中。

2. 切勿向任何人透漏或写下您的网上银行密码

ANS：

您应该是唯一知道您的网上银行密码的人。请确实保密您的网上银行密码，避免书写于实体卡片上，切勿向任何人透露。

3. 养成定期更改网上银行密码的习惯

ANS：

基于保障客户使用本行网上银行的安全，您的签入密码及转帐密码，最少一年内须变更，且到期前一个月，在您签入网上银行时，提醒您作密码变更、避免重复使用相同密码，并限制您的密码不可与您身分证字号相同。

4. 设定网上银行密码时提高警觉

ANS：

① 您必须清楚知道每一个与您共用电脑的人，同时严格限制任何未经授权人士使用您的电脑，并且必须安装个人防火墙及病毒测试软体。

② 为了预防您离开电脑过久，以至遭他人窃用，若您欲离开本行网上银行，敬请务必执行签退，并关闭浏览器，以保障您的权益及账户安全。本系统会在您逾十分钟未做任何交易时，自动执行签退网上银行服务。

5. 避免提供个人资料及金融资料

ANS：

一般的电子邮件与网页并没有受到安全加密的技术保护，当您无法确认传输的资料可受到网络安全机制的保护，千万不要向任何人透露您的密码。无论在任何情况下，本行不会询问客户的密码，因此您接获任何人

士的询问，请不必理会，若您需要与本行连络，请直接拨打本行客服专线：

中国大陆地区：86-755-25832208 转存汇部门【服务时间：深圳分行营业时间（周一至周五 9:00~15:30）】；

台湾地区/其它海外地区：886-2-2181-0101【服务时间：24 小时】。

6. 避免在公共电脑及网吧上进行任何网上银行交易

ANS：

①当您在公共场所使用电脑时，要记得确实签退「网上银行」并关闭浏览器，以避免藉由浏览器回上一页的功能，而泄漏资料予第三人。

②请您不要勾选"记住"「身分证字号/统一编号/网银识别代码」和「代号」的功能，以避免泄漏资料予第三人。

7. 确实核对网址

ANS：

①当您利用网上银行交易时，在登入网银时应留意核对所登入的网址，以避免不慎进入假网站。本行之个人网上银行网址为 https://netbank.hncb.com.tw、企业网上银行网址为 https://ibank.hncb.com.tw，https 是有「s」加密保护的喔！本行网上银行是采用 SSL 128bits 最高安全等级加密，以确保客户的资料在网络上是以加密的机制传输。请多自行输入本行网址，以避免进入骇客仿冒本行之网站，骗取账户信息。

②您可使用浏览器「加到我的最爱」功能，增加以后使用的方便性，并避免通过邮件或其它网站提供的连结登入。您亦可在签入网上银行之前，在浏览器页面连续两次点选金钥小图示，检视此认证是否为发给本行之"netbank.hncb.com.tw"或"ibank.hncb.com.tw"有效认证，以确保进入本行之网站。

8. 妥善保管交易明细表

ANS：

只要您透过网上银行进行任何的网络动作，如：转帐、查询和支付等交易，应保存最后执行动作的资料或予以记录，如发现异常交易或帐务差错，立即与本行联系，出示网络纪录，避免造成损失。

9. 远离来源不明的电子邮件

ANS：

您也许会收到像似好友或是公司的电子邮件，但是事实上有些伪造的电子邮件很有可能会让你在不知情的情况下，下载病毒程式或是木马程

式，或是将您引导到一个伪造的银行网站。因此切勿阅读与开启不明电子邮件的附件档案。

10. 其它注意事项

ANS：

(1)请勿将您的密码揭露予他人。

(2)请安装防毒软体及防火墙，并随时将防毒软体及防火墙更新至最新状态，以保护您的电脑避免遭受病毒或恶意程式入侵。

(3)请关闭档案及印表机分享设定，以避免个人或公务资料外泄，及被植入木马程式的风险。

(4)请考虑将您的个人隐私等敏感性资料或重要资料使用加密技术（例如：档案加密…）加以保护。

(5)请不要安装来源不明的软体或程式。

(6)请删除垃圾邮件或连锁信，也不要打开来自陌生人的电子邮件附件，以避免骇客入侵您的电脑，窃取个人资料。

(7)请勿将您的个人、财务或信用卡等资料留于不熟悉或有安全疑虑的网页。

(8)请定期备份重要的资料。

(9)请勿使用不能信任的电脑或设备。

(10)签入网上银行时应核对您上次签入的网络位址和时间，如有任何疑虑，请立即与本行联系。

(11)执行网上银行交易后，应检查您的帐上余额，如有任何疑虑，请立即与本行联系。

(12)本行网上银行采用高安全性的 EV SSL，若您看到 SSL 服务器凭证的警告讯息时(例如：此网站的安全性凭证有问题…)，请确认连结网址的正确性，如有任何疑虑，请立即与本行联系。

(13)交易完毕后请按「登出」按钮退出网上银行，以确保您真的签退成功。

(14)离开网上银行后，请关闭浏览器，避免有人利用浏览器回上一页的特性，偷窥您查询过的历史资料。

(15)为确保您享受到最高水平的安全性，您应使用最新版本的浏览器，以支持 SSL 128 bits 加密或更高的加密标准。

◎ 小心网络钓鱼（Phishing）

Phishing 与英文「fishing」（钓鱼）发音相同，两者意义也差不多。若引用直接中文典故：「姜太公钓鱼，愿者上钩」是最佳翻译。

网络钓鱼是一种新兴网络诈骗手法,多半是利用伪造电子邮件与网站作为「诱饵」，轻则让使用者不自觉泄漏个人资料，成为垃圾邮件业者的名单；严重一点，电脑可能会被植入木马程式，破坏系统或让重要信息遭窃。而最危险的情况是：诱骗使用者的银行账号密码、信用卡号与公民身份号码（身分证字号）等机密资料，钓鱼者再伺机偷窃金钱或有价信息。

网络钓鱼所用的诱饵千奇百怪，包括伪装成知名银行或在线服务业者通知使用者资料过期、无效需要更新，或者是基于安全理由进行身分验证，要求使用者重新确认银行账号密码或信用卡号。只要使用者一时不察经由电子邮件指引的网址，连结伪造得一模一样的账号登录页，就成了数位版姜太公手中「愿者上钩」的肥美大鱼。

如果您发现钓鱼网站，或者有任何疑虑，请立即与本行联系。

◎ 小心诈骗邮件

诈骗集团常假冒银行名义发出难辨真伪的电子邮件，如您收到此类信件，请主动提供此类不法信件予本行。

☆ 提醒您：

华南银行绝对不会寄发电子邮件要求客户揭露账户信息或任何密码,请提高警觉，千万不要回复此类邮件，并立即删除。若有任何问题或收到任何可疑邮件，请随时与本行客服中心联络：

中国大陆地区：86-755-25832208 转存汇部门【服务时间：深圳分行营业时间（周一至周五 9:00~15:30）】;

台湾地区/其它海外地区：886-2-2181-0101【服务时间：24 小时】。

1. 什么是诈骗邮件

ANS:

所有的网络使用者都应该了解什么是诈骗邮件，虽然它们难以辨识，但一般的诈骗邮件通常都会要求您点选一个连结网址并将您引导到一个

仿造的假网站，然后再要求您提供、更新或确认机密的个人资料；为了让您上当，他们也许会明示或暗示您现在发生了一个可能威胁到您账户的紧急情况。

☆ **提醒您：造假诈骗邮件希望获取的资料：**

- ＊ ATM 密码或预借现金密码。
- ＊ 信用卡有效号码。
- ＊ ATM/信用卡、现金卡卡号。
- ＊ 公民身份号码（身分证字号）。
- ＊ 银行账号。
- ＊ 网上银行签入代号及密码。

2. 辨识诈骗邮件

ANS：

①登入某冒用伪造的网上银行时，除 ATM 卡号及密码外，还要求您输入其它机密资料。

②寄发紧急、有时间限制或是要求您提供、更新或确认机密资料（如：登入用的使用者代号或密码、公民身份号码（身分证字号）、ATM/信用卡、现金卡卡号与密码或信用卡到期日）的电子邮件；或要求您在 e-mail 的空格内，填入机密的个人或账户资料。

3. 辨识诈骗邮件

ANS：

假如您收到造假诈骗邮件，请随时与本行联络，并将诈骗邮件提供给我们；将有助于我们加紧调查、杜绝这些诈骗邮件，防止更多人受骗。

☆ **提醒您：**

假如您无法认出某笔特定交易内容，或怀疑有人正在窃取您的账户资料，请立即与本行联络。

◎ 网络诈骗问答集（Q&A）

Q：何谓网络诈骗邮件？

ANS：

网络诈骗邮件就是仿造银行的规范与设计，事实上却是在网络上行使诈

骗密码与窃骗个人资料的不法份子所设计的圈套，这些冒用银行名义所发出的电子邮件，似乎让使用者也难辨真伪。提醒您千万不要回应，并马上删除。

Q： 收到要求更新网上银行密码及资料的不明来源邮件时，应如何处理？

ANS：

当您收到难辨真伪邮件时，除请在第一时间通知本行，并请马上删除此种邮件，千万不可回复，以免上当到造成损失。

Q： 我该如何保护自己？

ANS：

很多人担心网上银行交易的安全性，事实上，只要好好保管您的网上银行账户名称及密码，确保您的电脑系统及软体设有保护装置，并在上网时提高警觉，就可以安心在网上银行进行交易。

Q：如何确保网上银行安全性？

ANS：

一．设定网上银行密码时提高警觉：

1. 避免选用容易被猜中的号码或字母组合，例如：出生年月日。
2. 切勿使用您在其它网络服务的账户名称及密码，例如电子邮件或网络简讯，以免被有心人士猜中。
3. 密码不可是连续数字，且不可使用重复的字元。

二. 切勿向任何人透露或写下您的网上银行密码：应该唯有您才是唯一知道您的网上银行密码的人。

三. 切勿向任何人透露或写下您的 OTP 之一次性密码。

四. 应妥善保管金融卡、OTP 安控卡，避免遭任何人持有、使用或毁损。

五. 养成定期更改网上银行密码的习惯，避免重复使用相同密码。

六. 保护您的电脑：您应清楚知道每一个与您共用电脑的人，同时严格限制任何未经授权人士使用您的电脑，并且必须安装防火墙软体及安装病毒检测软体。

七. 避免在公共电脑及网吧上进行任何网上银行交易。

八. 避免提供个人资料与金融资料。

◎ 貼心的小叮咛：四勿三要

四勿

- 勿使用具有连贯性等容易被有心人猜到的数字设定密码。
- 勿向任何人透露或写下您的网上银行代号、签入密码及 OTP 产生的一次性密码。
- 勿提供个人资料及金融资料予他人。
- 勿在公共电脑及网吧上进行任何网上银行交易。

三要

- 要定期更改网上银行密码。
- 收到不明来源可疑邮件，请您立即通知华南银行。
- 要妥善保存交易明细表。