

對客戶使用電子銀行及相關電子服務的網絡安全保安建議

- 一、應切記不可向任何人透露其身份證號(ID)或密碼，尤其密碼函正本使用後應即銷燬，身份證號(ID)或密碼應牢記腦中，如要謄寫或記錄，則應加掩飾並妥為收藏。
- 二、密碼應勿選用與自己個人資料有關的號碼或英文字，例如出生日期、姓名、電話號碼、其他熟悉名稱，或以前用過的密碼，最好選用一個別人不易猜測到的密碼。
- 三、第一次進入網路銀行系統後，應立即更改密碼。
- 四、應定期更改密碼，如認為密碼已被破解應即通知本分行。
- 五、勿使用電子郵件等之連結，應自行於瀏覽器輸入本行網路銀行網址。
- 六、應避免在使用網路銀行服務中途離開電腦。
- 七、使用完畢應即登出網路銀行系統。
- 八、與他人共用電腦時，須特別謹慎小心，應將憑證資料、記憶體或個人電腦硬碟的臨時檔案刪除，因臨時檔案可能存留如帳號之類的敏感資料。
- 九、為避免攻擊者非法取得密碼，對可疑電郵應謹慎注意，因攻擊者可能秘密安裝程式盜取密碼。
- 十、切勿在公共場所 (如網咖) 使用網路銀行服務，因很難確保這些地方的電腦不會被有心人士安裝駭客程式，藉機盜取帳戶及密碼等資料。
- 十一、請注意無論在任何情況下，本行任何人員都不會以各種形式要求客戶透露網路銀行帳戶密碼。
- 十二、應經常檢查帳戶餘額、對帳單及網銀使用情形 (如上次網銀簽入日期及時間、公司戶有關編輯、核准及放行之授權設定與網路銀行之約定內容等)，始能及早發現是否有異常交易。
- 十三、遠離來源不明的電子郵件。
- 十四、請勿將您的一次性(OTP)密碼揭露予他人。
- 十五、請安裝防毒軟體及防火牆，並隨時將防毒軟體及防火牆更新至最新狀態，以保護您的電腦避免遭受病毒或惡意程式入侵。
- 十六、請關閉檔案及印表機分享設定，以避免個人或公務資料外洩，及被植入木馬程式的風險。
- 十七、請考慮將您的個人隱私等敏感性資料或重要資料使用加密技術 (例如：檔案加密...) 加以保護。
- 十八、不要安裝來源不明的軟體或程式。
- 十九、請刪除垃圾郵件或連鎖信，以避免駭客入侵您的電腦，竊取個人資料。
- 二十、請勿將您的個人、財務或信用卡等資料留於不熟悉或有安全疑慮的網頁。