保安提示

Contents

1 Internet Banking Security Tips 2
1.1 我們為保護您的安全做了什麼？ 2
1.2 你可以做些什麼來保護自己呢？ 2
1.2.1 密碼保護 2
1.2.2 詐騙網站 3
1.2.3 惡意軟體 3
1.2.4 未經授權的訪問 4
1.2.5 其他防護措施 4
2 Public Website Security Tips 5
2.1 保護私人密碼 5
2.2 偽冒網站 6
2.3 惡意軟件 7
2.4 未獲授權者侵襲 7
2.5 其它預防措施 8
2.6 流動理財保安 10
2.7 銀行卡保安提示 10

中国建设银行(亞洲)
China Construction Bank (Asia)

保安提示

1 Internet Banking Security Tips

1.1 我們為保護您的安全做了什麼？

- 通過使用 128 位安全套接字層（SSL）加密，我們確保您的資料在傳輸過程中的安全。
- 我們的系統會監視每個登錄嘗試。如果有多個連續的不正確的密碼嘗試登錄，線上服務將會暫停。
- 我們不會通過電子郵件或短信詢問客戶的賬戶號碼，密碼或任何個人資訊。
- 我們的伺服器擁有防火牆系統的保護，可以防止未經授權的訪問。
- 當您需要進行高風險的網上交易時，中國建設銀行（亞洲）網上企業銀行會提供雙重身份核實的驗證工具之一的一次性密碼（OTP）或身份驗證令牌來進行進一步確認。
- 一旦發生任何高風險交易，我們將立即通知您。

1.2 你可以做些什麼來保護自己呢？

1.2.1 密碼保護

密碼功能是保護您享受中國建設銀行（亞洲）網上企業銀行的關鍵。您需要仔細保護您的客戶號碼，用戶名稱和密碼。請認真考慮以下建議：

- 銷毀印有您密碼原始單據
- 當您第一次訪問網上銀行服務時更改您的初始密碼
- 定期更改您的密碼, 建議為 90 天
- 使用數位，大寫字母和小寫字母的組合為您的密碼
- 避免使用容易地被他人猜到的號碼或姓名，例如出生日期，身份證號碼或電話號碼
- 不要使用可由一般黑客程式拆解的密碼,如常見單字(Password)或易於識辨的鍵次組合(如 qwerty, etc)
- 避免將相同的密碼用於不同的網路服務賬戶和系統
- 切勿在電話中讀出你的密碼
- 切勿將您的密碼透露給任何人，包括建亚的工作人員
- 切勿不加掩藏寫下或記錄任何客戶號碼，用戶名稱和密碼
- 切勿在電子郵件內容中包含或發送您的客戶號碼，用戶名稱和密碼
- 當您使用客戶號碼，用戶名稱和密碼時確保沒有人在看
- 隨時留意你的保安裝置，以避免未經授權的第三方使用這樣設備進行網上交易。

1.2.2 詐騙網站

詐騙者可能發送偽造的電子郵件或短信，假裝是從中國建設銀行（亞洲）股份有限公司發出的。多數情況下這些郵件或短信看上去像真的來自銀行。

郵件或短信中會要求收件人輸入自己的個人資訊，如他們的用戶名稱，密碼，信用卡號碼等。

詐騙者通過這些電子郵件或短信指導收件人通過訪問包含在郵件或短信中的詐騙網站的超連結，要求用戶輸入他們的個人資訊和賬戶資訊。

請注意，銀行絕不會要求客戶通過電子郵件提供任何機密資料，所以不要回應任何可疑的、要求提供類似資訊的電子郵件或短信，或單擊其中所含的超連結。

如何預防？

- 在登入及輸入任何保密資料前，請必須確保您是透過分別 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手機版進入本行的官方網站
- 不要使用藏於電郵內的超連結直接進入網站，您應在瀏覽器內的網址列內直接輸入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用書簽
- 核實網站伺服器數位驗證（即瀏覽器網址列之「安全鎖」標誌）
- 經常更新您的防毒軟體並定期更改登入私人密碼
- 避免使用公共網絡登錄 網上銀行/手機銀行

1.2.3 惡意軟體

惡意軟件是不同類型的惡意程式碼的一個統稱。惡意程式碼的例子包括了電腦病毒、蠕蟲、特洛依木馬、間諜軟件及廣告程式和勒索軟件。潛在的損害可以包括資料的修改、破壞或竊取，允許未經授權的系統接達及執行非用戶想要的功能。

如何預防？

- 不要使用公用電腦或移動設備登錄到中國建設銀行（亞洲）網上企業銀行
- 不要下載任何來源可疑的程式或軟體到您的電腦，或開啟來歷不明的超連結及附件，或開啟包含於惡意文字短訊或多媒體短訊內的超連結及附件。
- 在您的電腦上安裝防病毒軟體和/或反間諜軟體程式，在下載程式或軟體或打開郵件之前運行該程式
- 定期更新您的防病毒軟體和/或反間諜軟體程式，並更改您的密碼
- 使用最新版本的操作系統、應用程式及瀏覽器

1.2.4 未經授權的訪問

為了保護您的電腦和它保存的擋，並阻止未經授權的訪問到您的電腦，您應該：

- 在您的電腦上安裝防病毒軟體和/或反間諜軟體，個人防火牆和安全補丁
- 安裝和定期更新防病毒軟體和/或反間諜軟體程式和安全補丁
- 下載程式或軟體，或打開電子郵件前運行防病毒軟體和/或反間諜軟體

1.2.5 其他防護措施

幫助您享受中國建設銀行（亞洲）網上企業銀行的一些有用安全提示：

- 完成操作後，請謹記登出
- 不要使用共用的電腦訪問您的中國建設銀行（亞洲）網上企業銀行
- 當你訪問你的網路賬戶服務時不要離開你的電腦和/或移動設備
- 每次登錄中國建設銀行（亞洲）網上企業銀行的官方頁面後都要檢查您上次訪問的日期和時間
- 審查非登記的第三方賬戶轉賬限額，並在必要時降低該限額
- 在每次通過網上銀行向非註冊賬戶進行資金轉移後，注意發送給您的短信通知
- 切勿安裝任何第三方提供的無法確定的應用程式
- 定期閱讀並遵循相關機構發佈的安全提示，例如：香港銀行公會，消費者委員會，香港警務處 (請參閱由香港警務處提供相關科技罪案資料 https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/types.html)，香港金融管理局，證券及期貨事務監察委員會或政府資訊科技總監辦公室等

2 Public Website Security Tips

2.1 保護私人密碼

私人密碼是您的「網上銀行」及「電話銀行」服務之鑰匙，因此您必須小心選擇及保護您的私人密碼。請仔細考慮以下之提議:

如何設定安全的密碼

- 使用以數字、大楷及小楷字母組成的「網上銀行」密碼
- 避免選取其他人能輕易猜中的數字或名稱，例如: 子女名字、寵物名字、生日日期或電話號碼
- 避免為各種不同網上服務賬戶及系統設定同一個私人密碼
- 定期更改您的密碼

如何安全地保存密碼

- 銷毀印有私人密碼的文件
- 切勿向任何其他人透露您的私人密碼或私人密碼的任何資料
- 切勿不加掩飾地寫下或記錄您的私人密碼
- 切勿記錄密碼在電腦、手機或當眼位置

如何安全地使用密碼

- 確保在沒有任何人士監察的情況下輸入您的私人密碼
- 未登出网上服務，切勿中途離開電腦
- 切勿透過電話讀出任何密碼
- 切勿將密碼包含在/或透過電郵訊息發出
- 在任何情況下，中國建設銀行(亞洲) 不會要求客戶提供賬户密碼和賬户名稱

2.2 偽冒網站

騙徒會做甚麼?

有些欺詐集團會假冒中國建設銀行(亞洲)股份有限公司傳送偽冒電郵，這些電郵看似來自真實的機構。

偽冒電郵可能會要求您輸入您的用戶姓名、私人密碼、一次性密碼（OTP）、信用卡號碼等。

此外，有些騙徒更會透過偽冒電郵內的超連結/ 二維碼引導您進入偽冒網站，並要求您輸入一些個人資料或戶口資料。

請注意，本行絕對不會要求客戶透過電子郵件提供保密資料，客戶如收到此等要求提供保密資料的可疑電郵，切勿回覆，亦切勿使用有關之超連結/ 二維碼。

如何防止?

- 在登入及輸入任何保密資料前，請必須確保您是透過分別 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手機版進入本行的官方網站
- 不要使用藏於電郵、互聯網搜索引擎或快顯視窗內的超連結/ 二維碼直接進入網站，您應在瀏覽器內的網址列內直接輸入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用書簽
- 核實網站伺服器數位證書（即瀏覽器網址列之「安全鎖」標誌）
- 檢查數位證書，以確保證書是發給“www.asia.ccb.com”或“intl.ccb.com”和證書還在有效期內
- 經常更新您的防毒及/或防間諜軟件並定期更改登入私人密碼

2.3 惡意軟件

甚麼是惡意軟件?

惡意軟件是不同類型的惡意程式碼的一個統稱。惡意程式碼的例子包括了電腦病毒、蠕蟲、特洛依木馬、間諜軟件及廣告程式和勒索軟件。潛在的損害可以包括資料的修改、破壞或竊取，允許未經授權的系統接達及執行非用戶想要的功能。

如何防止?

- 切勿從不明來歷的來源下載任何程式或軟件在您的電腦上，或開啟來歷不明的超連結及附件，或開啟包含於惡意文字短訊或多媒體短訊內的超連結及附件。
- 在您的電腦上安裝防毒及/或防間諜軟件程式，並於下載程式或軟件或開啟電郵前，應先執行有關程式
- 定期更新您的防毒及/或防間諜軟件程式，並經常更改您的私人密碼
- 使用最新版本的操作系統、應用程式及瀏覽器
- 切勿使用公共/ 共享的電腦或流動裝置登入「網上銀行」
- (請參閱由香港金融管理局提供相關科技罪案資料 https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/)

2.4 未獲授權者侵襲

為了保護您的電腦及所載的內容，並阻止未獲授權者進入您的電腦，您應該:

- 於您的電腦及/或流動裝置內安裝防毒及/或防間諜軟件程式，個人防火牆及安全更新
- 於下載程式或軟件或開啟電郵前，先執行防毒及/或防間諜軟件程式
- 定期更新防毒及/或防間諜軟件程式及安裝安全更新
- 請將您的客戶名稱及私人密碼保密
- 每次登入後查閱您最近一次登入本行官方網上銀行網站的日期及時間
- 每次使用網上服務後，請謹記登出
- 不時查核您的賬戶，並及時查閱銀行發出的提示訊息及結單
- 選擇以手機短訊收取的一次性專用密碼作為核證以使用網上證券買賣服務

2.5 其它預防措施

謹慎使用網上銀行服務

- 避免使用公共/ 共用的電腦、流動裝置或公共無線網絡登入網上銀行服務
- 每次登入後查閱你最近一次登入本行官方網上銀行網站的日期及時間
- 當您仍然使用網上銀行服務時，切勿離開你的電腦及/或放下您的手機不顧
- 每次使用網上服務之後，請謹記登出
- 評估您轉賬至非登記賬戶的限額，如有需要可降低其金額
- 本行與任何第三者聚合器流動應用程式都概無連繫，客戶不應向第三者披露其網上理財登入資料
- 避免安裝不明來歷的第三者聚合器流動應用程式
- 使用信譽良好的電腦保養/維修服務商
- 客戶需提供一個有效的手提電話及聯絡號碼，以作通知用途。如果有任何更改，請儘快通知本行
- 切勿安裝從第三者獲取而未經確定其安全性的應用程式

留意銀行訊息

- 請留意透過「網上銀行」轉賬至非登記賬戶後發送給您的手機短訊通知
- 若遇任何可疑或透過短訊形式接受多個「一次性專用密碼」，請立即與我們聯絡
- 及時查閱本行發出的訊息並查核交易紀錄
- 請不要將手機短訊收取的「一次性專用密碼」轉傳至其他手提電話號碼
- 若您懷疑您的網頁服務曾被其他人使用或發覺不尋常之交易，請即致電我們的「電話銀行」277 95533 或信用卡 24 小時客戶服務熱線 317 95533

其他相關資訊

- 有關香港金融管理局對「使用網上銀行的主要保安提示」所發行的電子小冊子，請按此了解更多。
- 有關香港銀行公會發行的參考刊物，請按此了解更多。

保安提示

「安心保證」

本行保障網上銀行服務客戶不會蒙受任何因第三者欺詐所導致之損失。若客戶方面並無嚴重疏忽、獨自，或與他人合謀進行不誠實、欺詐或犯罪行為，並於懷疑或發現任何欺詐行為時，立即向銀行舉報未受權之交易，您將毋須承擔任何未經您知情，同意或受權而經其網上銀行戶口現金支出的損失。然而，本行保障所涵蓋的金額僅限於從您的帳戶中非法轉移的金額。我們不會承擔任何其他損失，包括間接或特殊損失，損害，費用，法律費用或機會損失。詳情請參閱電子理財服務的有關條款和條件。

確保網上銀行保安完善需要客戶與銀行攜手努力，您的合作是同等重要。請您細心閱讀及採用以下預防措施，讓您盡享安全可靠的網上銀行服務。

2.6 流動理財保安

安全使用二維碼交易

- 掃描二維碼前要提高警覺，並確保來源可靠
- 確認付款前應先行核實每宗交易的付款詳情，付款後立即核實銀行發出的交易記錄
- 二維碼內可能會記錄您的個人資料。請在有需要的情況下才向第三方展示您的二維碼。
- 如需要於店內展示商戶二維碼，例如張貼於收銀台等，商戶應提高警覺，防止第三方更換或修改該二維碼。

提防 SIM 卡偷換

- 如您發現異常長時間未收到任何電話或短訊，請提高警覺。
- 如您懷疑您已成為 SIM 卡偷換騙局的受害者，請立即與您的移動服務提供商聯繫。
- 保護您的移動服務平台，以避免騙徒啟用短訊轉發服務或查詢短訊內容。
- 如您接到許多不明電話，請不要關掉手機。這可能是使您關掉手機的一種策略，以防止您注意到連線已被篡改。

2.7 銀行卡保安提示

其他相關資訊

- 有關香港金融管理局對「使用網上銀行的主要保安提示」所發行的電子小冊子，請按此了解更多。
- 有關香港銀行公會發行的參考刊物，請按此了解更多。
- 如您未有遵守以上保安貼士及未有於合理時間內通知本行，及/或有欺詐或嚴重疏忽的行為，您便須承擔所有因卡被盜用而引致的損失。
- 請緊記查閱本行提供的有關保安建議。