保安提示

Contents

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

保安提示

1 Internet Banking Security Tips

1.1 我们为保护您的安全做了什么？

- 通过使用 128 位安全套接字层（SSL）加密，我们确保您的资料在传输过程中的安全。
- 我们的系统会监视每个登录尝试。如果有多个连续的不正确的密码尝试登录，线上服务将会暂停。
- 我们不会通过电子邮件或短信询问客户的账户号码，密码或任何个人资讯。
- 我们的伺服器拥有防火墙系统的保护，可以防止未经授权的访问。
- 当您需要进行高风险的网上交易时，中国建设银行（亚洲）网上企业银行会提供双重身份核实的验证工具之一的一次性密码（OTP）与或身份验证令牌来进行进一步确认。
- 一旦发生任何高风险交易，我们将立即通知您。

1.2 你可以做些什么来保护自己呢？

1.2.1 密码保护

密码功能是保护您享受中国建设银行（亚洲）网上企业银行的关键。您需要仔细保护您的客户号码，用户名称和密码。请认真考虑以下建议：

- 销毁印有您密码原始单据
- 当您第一次访问网上银行服务时更改您的初始密码
- 定期更改您的密码, 建议为 90 天
- 使用数位，大写字母和小写字母的组合为您的密码
- 避免使用容易地被他人猜到的号码或姓名，例如出生日期，身份证号码或电话号码
- 不要使用可由一般黑客程式拆解的密码,如常见单字(Password)或易于识辨的键次组合(如 qwerty, etc)
- 避免将相同的密码用于不同的网路服务账户和系统
- 切勿在电话中读出你的密码
- 切勿将您的密码透露给任何人，包括建亚的工作人员
- 切勿不加掩藏写下或记录任何客户号码，用户名称和密码
- 切勿在电子邮件内容中包含或发送您的客户号码，用户名称和密码
- 当您使用客户号码，用户名称和密码时确保没有人在看
- 随时留意你的保安装置，以避免未经授权的第三方使用这样设备进行网上交易。

1.2.2 诈骗网站

诈骗者可能发送伪造的电子邮件或短信，假装是从中国建设银行（亚洲）股份有限公司发出的。多数情况下这些邮件看上去像真的来自银行。

邮件或短信中会要求收件人输入自己的个人资讯，如他们的用户名称，密码，信用卡号码等。

诈骗者通过这些电子邮件或短信指导收件人通过访问包含在邮件中的诈骗网站的超连结，要求用户输入他们的个人资讯和账户资讯。

请注意，本行绝对不会要求客户透过电子邮件或短信提供保密资料，客户如收到此等要求提供保密资料的可疑电邮或短信，切勿回覆，亦切勿使用有关之超连结/ 二维码。你应该马上删除它们。

如何预防？

- 在登入及输入任何保密资料前，请必须确保您是透过分别 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手机版进入本行的官方网站
- 不要使用藏於电邮内的超连结直接进入网站，您应在浏览器内的网址列内直接输入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用书签
- 核实网站伺服器数位验证（即浏览器网址列之「安全锁」标志）
- 经常更新您的防毒软件并定期更改登入私人密码
- 避免使用公共网络登录 网上银行

1.2.3 恶意软体

恶意软件是不同类型的恶意程式码的一个统称。恶意程式码的例子包括了电脑病毒、蠕虫、特洛依木马、间谍软件及广告程式和勒索软件。潜在的损害可以包括资料的修改、破坏或窃取，允许未经授权的系统接达及执行非用户想要的功能。

如何预防？

- 不要使用公用电脑或移动设备登录到中国建设银行（亚洲）网上企业银行
- 不要下载任何来源可疑的程式或软体到您的电脑，或开启来历不明的超连结及附件，或开启包含于恶意文字短讯或多媒体短讯内的超连结及附件。
- 在您的电脑上安装防病毒软体和/或反间谍软体程式，在下载程式或软体或打开邮件之前运行该程式
- 定期更新您的防病毒软体和/或反间谍软体程式，并更改您的密码
- 使用最新版本的操作系统、应用程式及浏览器

1.2.4 未经授权的访问

为了保护您的电脑和它保存的挡，并阻止未经授权的访问到您的电脑，您应该：

- 在您的电脑上安装防病毒软体和/或反间谍软体，个人防火墙和安全补丁
- 安装和定期更新防病毒软体和/或反间谍软体程式和安全补丁
- 下载程式或软体，或打开电子邮件前运行防病毒软体和/或反间谍软体

1.2.5 其他防护措施

帮助您享受中国建设银行（亚洲）网上企业银行的一些有用安全提示：

- 完成操作后，请谨记登出
- 不要使用共用的电脑访问您的中国建设银行（亚洲）网上企业银行
- 当你访问你的网路账户服务时不要离开你的电脑和/或移动设备
- 每次登录中国建设银行（亚洲）网上企业银行的官方页面后都要检查您上次访问的日期和时间
- 审查非登记的第三方账户转账限额，并在必要时降低该限额
- 在每次通过网上银行向非注册账户进行资金转移后，注意发送给您的短信通知
- 切勿安装任何第三方提供的无法确定的应用程式
- 定期阅读并遵循相关机构发布的安全提示，例如：香港银行公会，消费者委员会，香港警务处(请参阅由香港警务处提供相关科技罪案资料 https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/types.html)，香港金融管理局，证券及期货事务监察委员会或政府资讯科技总监办公室等

2 Public Website Security Tips

2.1 保护私人密码.

私人密码是您的「网上银行」及「电话银行」服务之钥匙，因此您必须小心选择及保护您的私人密码。请仔细考虑以下之提议:

如何设定安全的密码

- 使用以数字、大楷及小楷字母组成的「网上银行」密码
- 避免选取其他人能轻易猜中的数字或名称，例如: 子女名字、宠物名字、生日日期或电话号码
- 避免为各种不同网上服务账户及系统设定同一个私人密码
- 定期更改您的密码

如何安全地保存密码

- 销毁印有私人密码的文件
- 切勿向任何其他人透露您的私人密码或私人密码的任何资料
- 切勿不加掩饰地写下或记录您的私人密码
- 切勿记录密码在电脑、手机或当眼位置

如何安全地使用密码

- 确保在没有任何人士监察的情况下输入您的私人密码
- 未注销网上服务，切勿中途离开计算机
- 切勿透过电话读出任何密码
- 切勿将密码包含在/或透过电邮讯息发出
- 在任何情况下，中国建设银行(亚洲) 不会要求客户提供账户密码和账户名称

2.2 伪冒网站

骗徒会做甚么?

有些欺诈集团会假冒中国建设银行(亚洲)股份有限公司传送伪冒电邮，这些电邮看似来自真实的机构。

伪冒电邮可能会要求您输入您的用户姓名、私人密码、一次性密码（OTP）、信用卡号码等。

此外，有些骗徒更会透过伪冒电邮内的超连结/ 二维码引导您进入伪冒网站，并要求您输入一些个人资料或户口资料。

请注意，本行绝对不会要求客户透过电子邮件提供保密资料，客户如收到此等要求提供保密资料的可疑电邮，切勿回覆，亦切勿使用有关之超连结/ 二维码。

如何防止?

- 在登入及输入任何保密资料前，请必须确保您是透过分别 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手机版进入本行的官方网站
- 不要使用藏於电邮、互联网搜索引擎或快显视窗内的超连结/ 二维码直接进入网站，您应在浏览器内的网址列内直接输入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用书签
- 核实网站伺服器数位证书（即浏览器网址列之「安全锁」标志）
- 检查数字证书，以确保证书是发给 “www.asia.ccb.com”或 “intl.ccb.com”和证书还在有效期内
- 经常更新您的防毒及/或防间谍软件并定期更改登入私人密码

2.3 恶意软件

甚么是恶意软件?

恶意软件是不同类型的恶意程式码的一个统称。恶意程式码的例子包括了电脑病毒、蠕虫、特洛依木马、间谍软件及广告程式和勒索软件。潜在的损害可以包括资料的修改、破坏或窃取，允许未经授权的系统接达及执行非用户想要的功能。

如何防止?

- 切勿从不明来历的来源下载任何程式或软件在您的电脑上，或开启来历不明的超连结及附件，或开启包含于恶意文字短讯或多媒体短讯内的超连结及附件。
- 在您的电脑上安装防毒及/或防间谍软件程式，并于下载程式或软件或开启电邮前，应先执行有关程式
- 定期更新您的防毒及/或防间谍软件程式，并经常更改您的私人密码
- 使用最新版本的操作系统、应用程式及浏览器
- 切勿使用公共/ 共享的电脑或流动装置登入「网上银行」
- (请参阅由香港金融管理局提供相关科技罪案数据 https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/)

2.4 未获授权者侵袭

为了保护您的电脑及所载的内容，并阻止未获授权者进入您的电脑，您应该:

- 于您的电脑及/或流动装置内安装防毒及/或防间谍软件程式，个人防火墙及安全更新
- 于下载程式或软件或开启电邮前，先执行防毒及/或防间谍软件程式
- 定期更新防毒及/或防间谍软件程式及安装安全更新
- 请将您的客户名称及私人密码保密
- 每次登入后查阅您最近一次登入本行官方网上银行网站的日期及时间
- 每次使用网上服务后，请谨记登出
- 不时查核您的账户，并及时查阅银行发出的提示讯息及结单
- 选择以手机短讯收取的一次性专用密码作为核证以使用网上证券买卖服务

2.5 其它预防措施

谨慎使用网上银行服务

- 避免使用公共/ 共用的电脑、流动装置或公共无线网络登入网上银行服务
- 每次登入后查阅你最近一次登入本行官方网上银行网站的日期及时间
- 当您仍然使用网上银行服务时，切勿离开你的电脑及/或放下您的手机不顾
- 每次使用网上服务之后，请谨记登出
- 评估您转账至非登记账户的限额，如有需要可降低其金额
- 本行与任何第三方聚合应用程序都没有联系，客户不应向第三方披露其网上理财登入资料
- 避免安装不明来历的第三者聚合器流动应用程序
- 使用信誉良好的计算机保养/维修服务商
- 客户需提供一个有效的手提电话及联络号码，以作通知用途。如果有任何更改，请尽快通知本行
- 切勿安装从第三者获取而未经确定其安全性的应用程式

留意银行讯息

- 请留意透过「网上银行」转账至非登记账户后发送给您的手机短讯通知
- 若遇任何可疑或透过短讯形式接受多个「一次性专用密码」，请立即与我们联络
- 及时查阅本行发出的讯息并查核交易纪录
- 请不要将手机短讯收取的「一次性专用密码」转传至其他手提电话号码
- 若您怀疑您的网页服务曾被其他人使用或发觉不寻常之交易，请即致电我们的「电话银行」277 95533 或信用卡 24 小时客户服务热线 317 95533

其他相关资讯

- 有关香港金融管理局对「使用网上银行的主要保安提示」所发行的电子小册子，请按此了解更多。
- 有关香港银行公会发行的参考刊物，请按此了解更多。

保安提示

「安心保证」

本行保障网上银行服务客户不会蒙受任何因第三者欺诈所导致之损失。若客户方面并无严重疏忽、独自，或与他人合谋进行不诚实、欺诈或犯罪行为，并于怀疑或发现任何欺诈行为时，立即向银行举报未受权之交易，您将毋须承担任何未经您知情，同意或受权而经其网上银行户口现金支出的损失。然而，本行保障所涵盖的金额仅限于从您的账户中非法转移的金额。我们不会承担任何其他损失，包括间接或特殊损失，损害，费用，法律费用或机会损失。详情请参阅电子理财服务的有关条款和条件。

确保网上银行保安完善需要客户与银行携手努力，您的合作是同等重要。请您细心阅读及采用以下预防措施，让您尽享安全可靠的网上银行服务。

2.6 流动理财保安

安全使用二维码交易

- 扫描二维码前要提高警觉，并确保来源可靠
- 确认付款前应先行核实每宗交易的付款详情，付款后立即核实银行发出的交易记录
- 二维码内可能会记录您的个人资料。请在有需要的情况下才向第三方展示您的二维码。
- 如需要于店内展示商户二维码，例如张贴于收银台等，商户应提高警觉，防止第三方更换或修改该二维码。

提防 SIM 卡偷换

- 如您发现异常长时间未收到任何电话或短讯，请提高警觉。
- 如您怀疑您已成为 SIM 卡偷换骗局的受害者，请立即与您的移动服务提供商联系。
- 保护您的移动服务平台，以避免骗徒启用短讯转发服务或查询短讯内容。
- 如您接到许多不明电话，请不要关掉手机。这可能是使您关掉手机的一种策略，以防止您注意到连线已被篡改。

2.7 银行卡保安提示

其他相关资讯

- 有关香港金融管理局对「使用网上银行的主要保安提示」所发行的电子小册子，请按此了解更多。
- 有关香港银行公会发行的参考刊物，请按此了解更多。

- 如您未有遵守以上保安贴士及未有于合理时间内通知本行，及/或有欺诈或严重疏忽的行为，您便须承担所有因卡被盗用而引致的损失。

- 请紧记查阅本行提供的有关保安建议。