

提防钓鱼讯息 保障信用卡安全

中国银行(香港)(「中银香港」)提醒客户及公众人士，慎防意图骗取个人资料及信用卡资料的钓鱼电邮/短讯。

近日有骗徒伪装网购平台/积分奖赏平台/邮政服务/速递公司/银行发出钓鱼电邮或短讯，以不同借口要求客户点击电邮或短讯内的超链接进行验证、付费或个人资料更新，例如讹称平台需客户更新数据才能继续提供服务，或客户有包裹因故无法派递而需更新数据及/或额外付费，诱骗客户在该超链接的伪装网站内输入个人及信用卡数据。

这些虚假电邮、短讯及伪装网站的超链接会以不同组合，甚至仿似相关机构真正网址的域名(如以类似的英文字母、数字或符号取代)出现，而虚假短讯的发送人名称有机会与真实商户名称相同，导致虚假短讯与过往来自真实商户的短讯共同显示，企图误导客户及盗取客户的个人及信用卡资料，从而用于非法用途，包括**绑定流动支付及服务**后，在本地或海外进行未经授权签账，或**直接以盗取的数据进行未经授权的网上交易**。

中银香港重申不会以电话、电话录音、电邮、短讯、超链接、二维码或附件等方式，索取客户的敏感个人资料，包括银行帐户数据、网上银行用户名称、登入密码、一次性密码或信用卡号码/保安码。

本行呼吁客户提高警觉，慎防受骗：

- 请小心保护个人资料，切勿向任何人透露敏感个人资料、信用卡数据、及任何密码，包括短讯一次性密码。
- 尽管现时流动装置具备自动填写一次性密码的功能(AutoFill)，请于输入有关一次性密码以进行任何交易授权前，小心核对一次性密码短讯的内容及交易

資料(例如：商户名称、交易类别、交易金额及货币)是否与实际进行的用途或交易相符。

- 输入任何数据或进行交易前，须检视该网页地址是否真确与可信。
- 切勿打开来历不明的电邮、短讯、附件或超链接及下载可疑的应用程序。如有怀疑，请即停止操作，切勿输入任何数据，关闭窗口，并向本行查询，或透过真实商户的官方联络途径核实。
- 如客户曾向怀疑伪冒网站提供数据，请即致电客户服务热线(852) 3988 2388（选取语言后，按 3、#、2），并向警方举报。
- 如客户收到有关绑定流动支付及服务或网上交易的可疑讯息，请立即报警求助及与本行联络。
- 经常透过网上银行、手机银行或月结单检查信用卡交易纪录以检查是否有任何可疑或未经授权的交易。

本行会不时于本行网页更新有关诈骗信息提示，详情请浏览 www.bochk.com/sc/aboutus/fraudalert.html。有关电子银行服务的保安信息，请浏览 www.bochk.com/sc/security.html。

中国银行(香港)有限公司谨启

2023 年 2 月 7 日