账户盗用

账户盗用

什么是帐户盗用?

此类诈骗一般由于骗徒诱导您泄露个人资料，从而取得您的银行账户存取权限。他们会重设密码及安全验证资料，使您无法登入账户，并可能更改账户所连结的电话号码、地址及电邮地址，令其可如同合法客户般操作账户。

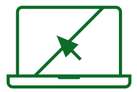
遥距账户盗用

此类诈骗是指骗徒控制您的装置某网站，并在您毫不知情或未经授权的情况下，从您的银行账户进行付款。骗徒通常会先发送连结、要求您浏览或下载特定软件，以取得您的装置的远端存取权限。透过阅读本指南，您将了解骗徒常用的手法，并掌握防范措施，保护自己及业务免受侵害。

电话号码诈骗

这是指骗徒透过更改来电显示号码，伪装成您的银行的官方电话号码。该号码可能与真实号码完全相同，或仅相差一个数字。骗徒亦可能使用隐藏号码来致电。

恶意程式与网络钓鱼



骗徒会利用恶意软件及连结窃取个人资料。

这些资料可能被用作诱导您误信某通电话属真实来电，或用以入侵您的银行账户。

授权代码

请注意：包括银行在内的任何机构，绝不会指示您如何使用实体或数码保安装置（即「保安编码」），亦不会要求您提供网上理财授权代码。.

账户盗用

建议贴士

- ✓ 切勿透露您的网上理财使用者名称、密码、授权代码或任何一次性密码 (OTP)。
- ✓ 请记住，来电号码有可能被伪造，切勿单凭来电显示判断对方身份。
- ✓ 如接获不明来历的电话，请挂线并改用经独立渠道核实的电话号码（例如对方官方网站所列的号码）回拨查询。建议使用另一部电话，或先联络熟悉的联络人，以确保通话线路安全无虞。
- ✓ 对可疑电邮及短讯务必提高警觉，尤其是含有连结或要求提供资料的讯息。所有要求提供资料的讯息，应直接向相关公司核实，并参照上述联络方式。
- ✓ 切勿因不明来历的电话而点击任何连结、浏览网站或下载软件。
- ✓ 您的保安编码装置属个人专用。如有人来电要求您使用该装置，请立即终止通话并联络您的银行。
- ✓ 恒生绝不会要求您参与任何正在进行的调查、指导您如何回答问题，或要求您将资金转至所谓「安全账户」。
- ✓ 请确保公司已设立既定程序，让员工通报可疑情况，并确保全体员工均了解「遥距账户盗用」诈骗的风险。
- ✓ 加强员工教育——确保所有人员均认识「遥距账户盗用」诈骗手法，并已建立相应的通报及处理流程。
- ✓ 在付款流程中建立严谨的尽职审查文化，例如采用双重审批机制，以加强风险防控。