



提防非接触式移动支付服务绑定或结合恶意软件及 NFC 功能的诈骗

近日有骗徒冒充商户或者机构发送钓鱼信息，诱导市民将支付卡（包括信用卡、扣账卡及提款卡）绑定至伪冒装置，或利用恶意软件结合手机近场通讯（NFC）功能进行未经授权的盗刷。

与蜜桃保保一起拆解骗徒手法：

手法一：钓鱼短信及假冒绑定卡

骗徒假冒商户发送短信，以「货品赔偿」等借口，诱骗市民输入银行卡资料及自动柜员机（ATM）密码后，在伪冒装置上绑定受害人的支付卡。一旦受害人批准绑定请求，骗徒即可进行盗刷。

手法二：恶意软件及 NFC 遥距读卡

骗徒诱骗市民下载来历不明的应用程序并获取手机权限后，诱导受害人将支付卡贴近手机，利用 NFC 功能遥距读取卡内信息并进行盗刷。

蜜桃保保防骗守则：

- 切勿回复或批准任何非本人发起的支付卡绑定请求，包括透过手机银行應用程式或双向短信发出的要求或交易，并仔细阅读银行信息及通知
- 切勿从不明网站下载或安装應用程式。本行绝不会要求客户把支付卡贴近手机背面作认证或解锁
- 切勿向陌生人透露银行密码、卡资料、或一次性验证码（OTP）等敏感个人资料，亦绝不点击信息或电邮中的可疑连结、二维码进行交易或提交资料

如客户收到怀疑伪冒本行发出的信息，请即致电中银香港客户服务热线（852）3988 2388（选取语言后，按 3、#、2）。