



提防「猜猜我是誰」騙案及偽冒政府醫療服務平台的釣魚短信

蜜桃蜜桃，勿信騙徒！作為中銀香港的防騙大使「蜜桃保保」，我時刻「一眼關七」，全力守護您的帳戶安全。為保障個人資產安全，蜜桃保保根據香港警務處近日提供的防騙資訊，為您整理以下關於「猜猜我是誰」騙案及偽冒政府醫療服務平台的釣魚短信的防騙提示，請務必提高警覺。

警惕「猜猜我是誰」騙案：無論多熟識 提到轉帳要警惕！



警方近期接获多宗「猜猜我是谁」骗案，个案呈上升趋势，长者受害人的损失由港币数千元至数万元不等。不少长者因较少接触防骗资讯，仅凭声线相似便相信对方身份。

三大骗徒手法：

1. 剧本型

- 非法取得市民资料后，量身订制冒充身份、转账借口，甚至模仿声线
- 致电／用聊天软件接触受害人，提出转账请求

2. 骑劫型

- 骑劫受害人聊天账户，透过翻阅历史对话掌握联络人身份、人际关系
- 在聊天账户向受害人的联络人提出转账要求

3. 白撞型

- 打电话与受害人闲话家常，但不说出自己是谁，诱导受害人猜测身份
- 一旦受害人猜测，骗徒便会马上冒认

近期个案：

(一) 一名退休人士接获陌生来电，骗徒自称「律师行职员」，指事主丈夫去年曾发生交通意外（意外为真实发生，骗徒非法取得事主个人资料），现正处理索偿事宜，要求先支付港币 2 万元「手续费」。事主未经查证便转账，结果受骗。

(二) 一名长者接获陌生来电，骗徒自称是「女儿」，指最近换了电话号码。因声线相似，事主未起疑心。翌日，骗徒再度致电，称需要资金周转，要求事主拿现金到指定屋苑交收。事主如约前往，见到一名中年男子自称代「女儿」收钱，事主致电骗徒确认后便将现金交出，结果受骗，损失约港币 3.5 万元。

(三) 一名工程师于即时通信软件接获「堂妹」信息，指急需港币 1.2 万元，并承诺后天归还。事主因工作忙碌，未经深究便转账至陌生银行账户。其后，骗徒再要求转账港币 8 万元，事主起疑，尝试以即时通信软件致电堂妹但无人接听。骗徒随即发送一段录音，再次催促转账。幸好事主提高警觉，改用手机号码联络堂妹，才揭发其即时通信软件账户已被盗用。

(四) 骗徒模仿声线致电一名退休人士，自称是其「侄仔」，指被警方拘留，急需港币 1 万元保释金。事主因声线相似而信以为真，按指示到便利店扫描支付平台二维码转账。当日事主致电侄女，才揭发是骗案，损失约港币 6,000 元。



中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

(五) 騙徒假扮电讯公司客服致电一名餐厅店员，讹称事主欠费港币 250 元，若不即时补交便要罚款港币 5,000 元。事主信以为真，按骗徒指示到银行柜员机转账，期间一直保持通话。事主转账港币 1 万元后，骗徒再要求转账港币 5 万元，事主起疑，立即报警求助。

警方呼吁：

- 遇突发转账要求，无论是否熟识对方、声线如何相似，都要进一步验证身份，例如亲自致电确认或会面。
- 骗徒常先搜集您的背景及家人资料，再冒充熟人，令骗局更逼真。
- 若来电者要求转账至平日不熟悉的银行账户，必须立即提高警惕。
- 针对没有电子银行的长者，骗徒可能建议由「朋友」或「律师」代收现金，切勿答应。
- 任何涉及金钱的要求，都要冷静求证，绝不匆忙转账。
- 多关心身边长者，定期分享防骗资讯。
- 若有怀疑，立即致电「防骗易 18222」热线查询。

提防假冒 HA Go 或 eHealth 钓鱼短信



警方接获多宗假冒「HA Go」或「eHealth」钓鱼短信报告。骗徒讹称事主的「自愿医保计划」、「大湾区港澳通医疗保障计划」、「港澳通医疗保障计划」或「跨境医疗保障计划」试用期结束，即将每月自动扣费，并留下电话号码诱骗市民回拨。

最新受害人包括医护人员及大学讲师，前者听从指示在假冒金融服务网站输入信用卡资料，随即被盗刷逾港币 6,000 元；后者误信转账是「取消计划程序」，损失近港币 34 万元。

医务卫生局（医卫局）及医院管理局（医管局）已作出严正声明：官方从未发出有关短信，并已就事件向警方报案。医健通和医管局已参与「短信发送人登记制」，所有官方的短信名称均以「#」号开头（例如 #HA Go 或 #eHealth），以便市民辨识。医管局如需致电市民，一般会由职员亲自来电并提供资料核实身分。同时，当局正分阶段转用 18285 或 18286 作为来电开头。

骗徒常见手法：

- 大量发放虚假短信，讹称医保计划到期及即将扣费，引诱市民回拨指定的联络电话。
- 假冒客服指示事主登入虚假网站，并输入银行或信用卡资料以「取消会籍」。
- 一旦骗徒取得个人及／或账户资料，随即盗刷信用卡或转走存款。



中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

五大提示：

1. 官方短信必有「#」号（#HA Go / #eHealth），无「#」号一律须提高警惕。
2. 切勿点击短信内连结、回拨不明电话，或向可疑网站提供任何个人及／或账户资料。
3. 骗徒可能讲流利广东话，甚至以视像通话「教导」转账，切勿相信。
4. 「服务试用期结束、即将自动扣费」是近期常见钓鱼短信诈骗手法，应提高警觉。
5. 如曾向可疑第三方提供个人及／或账户资料，立即联络银行冻结相关账户以减少损失，并报警求助。

警方呼吁：

- 切勿点击可疑短信内的连结或回拨电话号码；
- 除了向有关机构验证外，市民亦可在守网者网站的「防骗视伏器」或「防骗视伏 App」应用程式输入可疑资料作即时查核；
- 如有怀疑，请立即致电「防骗易 18222」热线查询。

中国银行(香港)有限公司 谨启

2026 年 9 月 25 日