甚么是网上账户骑劫？

早在2014年，已经出现户口骑劫案件。当时，实时通讯软件LINE由于有系统漏洞，导致用户账号被黑客入侵并骗取通讯簿的亲友购买点数卡，有关漏洞直至大约2016年才得以修复。在2017年，有骗徒开始骑劫用户的WhatsApp帐户，亦以同样手法骗取市民购买点数卡，后来WhatsApp推出「双步骤验证」（现称「双重验证」）功能，情况才逐步得以改善。

2023年8月开始出现新型账户骑劫手法。新手法利用钓鱼白撞讯息，后来演变为「搜寻器优化中毒」的攻击。当中大部分的案件涉及WhatsApp账户，亦有小量涉及Telegram和其他网上平台。

手法一：钓鱼短讯

- 骗徒发送钓鱼短讯，内附连结至假网站
- 假网站套取用户电话号码，并要求平台向用户发放转移代码
- 骗徒再向用户套取转移代码
- 骗徒用另一装置登入用户的帐户
- 骗徒向用户的亲友以转账或借贷为名骗财

手法二：搜寻器优化中毒攻击

- 骗徒制作假WhatsApp网页登入版面网站
- 骗徒在搜寻器以「WhatsApp」作为关键词投放广告
- 用户在搜寻器输入关键词「WhatsApp」，假网站便会以置顶广告形式出现
- 用户点击置顶广告进入虚假网站，然后扫描恶意二维码，骗徒随即取得用户联机数据
- 骗徒经网上版WhatsApp同时登入用户的帐户，并向亲友骗财

其实，网上账户入侵可能有不同的原因，例如曾在公用计算机上登入网页版的实时通讯软件而忘记注销、使用了恶意的多帐户登入工具、电子装置遭到恶意软件入侵等。

骗徒通常以网上银行转账超出限额为由，要求通讯簿的联络人帮忙转钱，并且承诺翌日还钱，要求转钱的数目也是由数千至数万元不等。当然偶尔也有巨额转账要求。

提防网上账户骑劫的贴士：

启用双重认证功能

定期检视帐户所链接的装置，并且注销所有不明的已链接装置

切勿随便透露密码、验证码或扫描二维码

于留言信箱设定强密码，避免一次性语音密码被盗取

避免连接公共Wi-Fi或在公共计算机上登入网上账号

不要尽信搜寻器的结果，建议将常用网页加入书签

留意短讯内容和网页是否有异样，例如域名串错字、繁简字夹杂等

如收到亲友透过讯息要求帮忙过数或汇款，应致电对方确认其身份及有关要求

如有怀疑，可在「防骗视伏器」输入网址、收款账号等评估风险，或致电18222查询