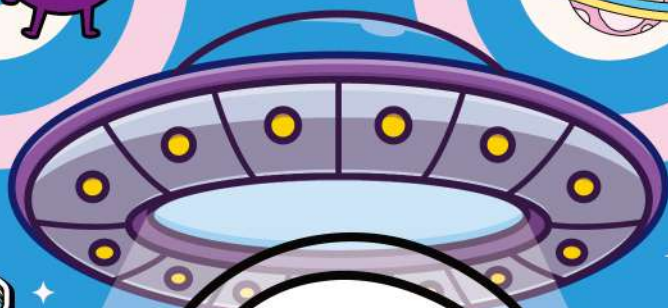




ADCC
Anti-Deception Coordination Centre
反诈骗协调中心



反击无限诈术

Understand
FactCheck
Outsmart
理解
查证
智破



全城 防骗手册

Your Scam

Prevention Manual



终极天书
All answers are
inside



14

种流行诈术 | 特征 | 防骗技巧

14 popular scams X characteristics X prevention techniques

WWW.ADCC.GOV.HK

2026年3月第二版

目录

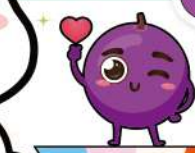
防骗热线一览

页数	内容
1	防骗热线一览
2	反诈骗协调中心简介
3-4	骗案排行榜
	本港常见骗案类型
	假冒身份篇
5-8	01 假冒官员
9-12	02 假冒客服
13-14	03 AI 换脸(deepfake)骗案
15-16	04 猜猜我是谁
17-19	05 假冒技术支持骗案
	网上交易篇
20-22	06 租屋骗案
23-25	07 钓鱼骗案
26-28	08 网上购物骗案
29-30	09 租/借/卖银行账户
	情感利诱篇
31-32	10 裸聊骗案
33-35	11 网上投资骗案
36-38	12 网上情缘骗案
39-41	13 「刷单赚佣」求职骗案
42-44	14 网上求职骗案(人口贩卖)
45	「骗案预警」计划
46	防骗视伏App

热线	功能
24小时「防骗易 18222」 谘询热线	查询最新诈骗手法 / 寻求意见 / 举报案件
紧急热线 999	情况紧急, 需要即时协助
个人资料隐私专员公署个人 资料防骗热线 3423 6611	处理怀疑骗取个人资料的 查询或投诉
香港网络安全事故协调中心 热线 8105 6060	接受与网络安全相关的 事故报告, 包括恶意程式、 网络钓鱼、网络诈骗等
入境事务处「协助在外香港居民 小组」24小时求助电话/ WhatsApp: +852-1868	境外求助
微信求助热线: 关注「香港入境事务处」 官方账号, 然后按 「1868 求助热线」联络小组	
香港警务处网页电子报案中心 https://crp.police.gov.hk/crp001?lang=sc	非紧急报案, 无需警方 即时协助

不确定是不是 **骗案**
 致电
18222 问我!

HOTLINE



反诈骗协调中心简介

Anti-Deception Coordination Centre (ADCC)

反诈骗协调中心(ADCC)隶属香港警务处商业罪案调查科，专门协调警队各部门打击及预防诈骗

工作重点

制定策略方针 提供电话咨询 多方协调
推行防骗宣传 监察骗案趋势 评估风险

设有24小时「防骗易18222」咨询热线

怀疑受骗，请尽快联络我们！

www.adcc.gov.hk/zh-cn/home.html





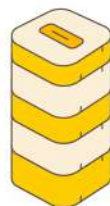
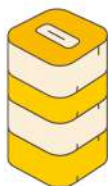
过去 3 年 骗案宗数
骗案数字 轻微下跌



+42.6%

+11.7%

-2.9%

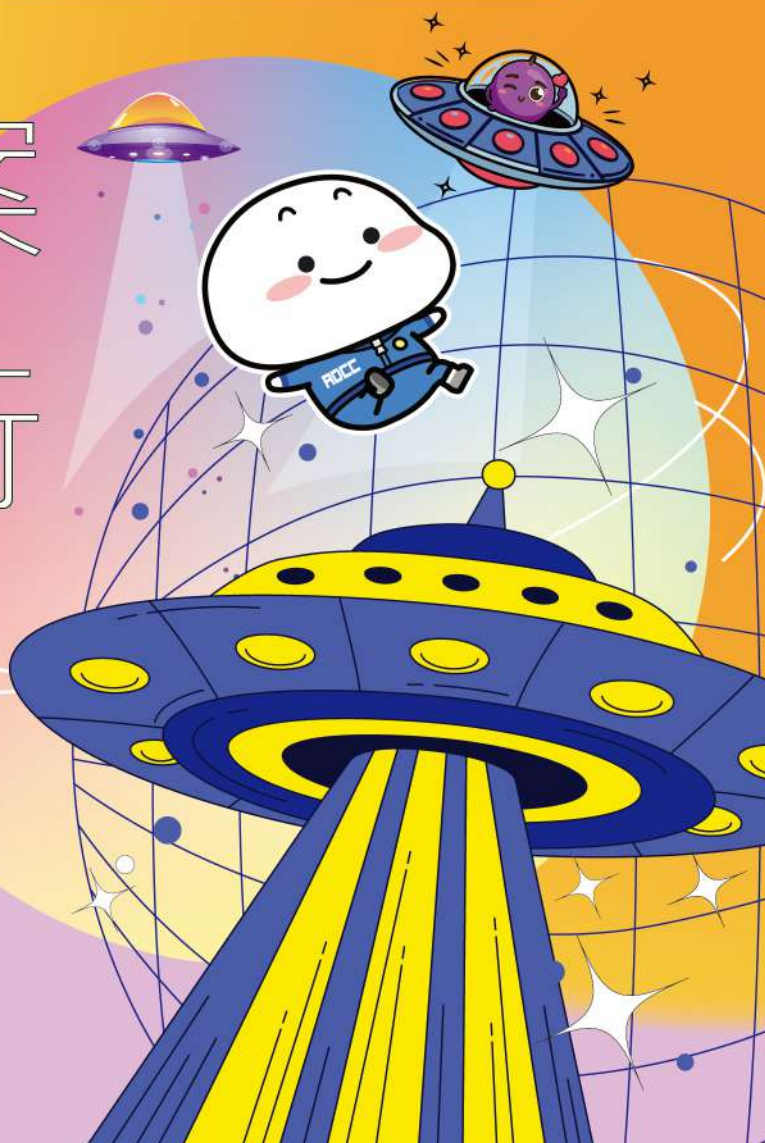


2023
39,824 宗

2024
44,480 宗

2025
43,212 宗

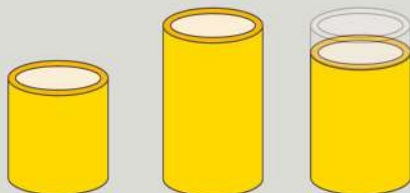
骗案 排行 榜





骗案金额 显著回落

-10.3亿



2023 91.8亿
2024 91.5亿
2025 81.2亿 (港元)

www.adcc.gov.hk

骗术排行榜

(2025年以案件宗数计)



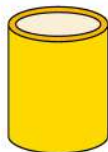
12,505宗 5,135宗 4,440宗



呃钱之最

(2025年以损失金额计)

第一位
网上投资骗案



35.8亿

第二位
假冒官员骗案



8.87亿

第三位
刷单骗案



8.6亿 (港元)



01

假冒身份篇

假冒官员



内地公安

来电指控 你犯法？



手法

假扮速递公司/电讯公司/银行/政府部门
以预录语音或真人致电



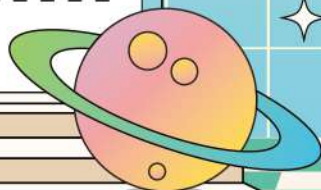
转驳至假冒内地执法人员
讹称你：

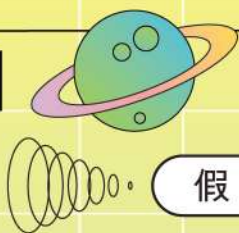
牵涉内地刑事案

开通了新电话号码，在内地散播危害国安信息

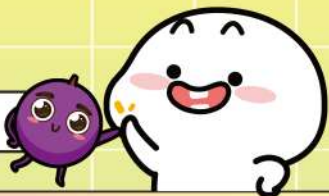


1. 要求转账「保证金」至指定账户
2. 要求下载手机应用程序 (App) 或在假网站输入银行理财密码，从而转走存款





假冒官员



真实案例（部分情节经过改动）

法律系学生为千元毁前程

23岁内地来港的硕士生陈小明(化名)某日被一个陌生电话直呼其名。

● 来电者：喂！陈小明，我是电讯公司职员，我们发现你的银行账户有问题！现在转驳去内地公安部，你积极配合调查吧！

★ 小明：什么？我什么都没做呀，我只是个普通学生
转驳后……

● 来电者：（普通话）你是陈小明？

★ 小明：我是……请问我的银行账户有什么问题呢？

● 来电者：（普通话）你听着，我们怀疑你和内地一宗洗钱案有关，如果你是清白的话，请配合我们调查，我们只给疑犯一次机会！



来电者要求小明转账20万元「保证金」以示清白，说会在查清资金来源后还给他。小明既惊又恐，对方再突然要求视讯通话，接听后屏幕出现一个身穿「公安制服」的男子，身后白墙赫然有「中国公安部」五个大字。小明还发现他手上有一张「拘捕令」，上面正正写着自己的名字。

男人用严肃语气向小明认真查问「案情」，指示小明在酒店见面，并叫他签署「保密协议」。不过，小明愈想愈不对劲：政府部门不是常说不会收保证金吗？于是致电18222问个究竟。

接报警员顺水推舟，在酒店陪小明等候「官员」现身。果然，一名穿西装的男子主动走近，马上被警员拘捕，身上被搜获多份伪造保密协议及伪造公安证件。

结局：

小明没有任何金钱损失，而被捕西装男子为就读法律系的本地大学生，被揭发为了赚取千元报酬而扮演官员行骗，自毁前程。

01

假冒身份篇

假冒官员

特征

身穿仿制公安制服

要求转账「保证金」

伪造拘捕令

声称帮你证明清白

威胁限制出入境

要求保密及断绝与外间联系



防骗图示



防骗技巧

- 若来电者自称「公安」，
立即挂断电话
- 紧记内地公安或执法人员
不会致电至香港办案
- 内地公安**绝不会**要求你
缴交「保证金」，
或提供银行资料及理财密码

冒充内地执法人员

见了证件也未必是真的

骗上骗



真实案例 (部分情节经过改动)

受害人变「特务」

骗徒在诱骗受害人转账后，会进一步怂恿他们参与所谓「特务行动」，并讹称完成任务后可取回被骗款项。

曾有受害人深陷假冒官员骗案，为求「赎罪」而同意担任「特务」，**按照骗徒指示**向其他受害人展示伪造的执法人员证件、假保密令并收取骗款。然而，市民明知而协助骗徒进行犯罪活动，同样需要**负上法律责任**。



刑责

根据《刑事罪行条例》
任何人使用或管有虚假文书
任何人士如干犯串谋欺诈罪行
一经循公诉程序定罪，
最高可处14年监禁



02

假冒身份篇

假冒客服

电讯商发短讯

要你填资料?

手法

骗徒假扮支付平台/大型企业(例如微信、淘宝、WhatsApp、YouTube、Netflix)/电讯商/银行的客服致电市民,部分发放钓鱼短讯



以不同借口诱导你回拨电话或点击钓鱼连结

常见借口:

- 声称你有大额保单,即将要以自动转账方式缴交保费
- 你有快递未能派送
- 你曾订购产品/服务但未付款,或会以月费形式从你户口扣除



指示输入网上理财用户名称、密码及验证码

然后转走你的存款



认清 NOTICE



= 骗钱!

遇到有人自称支付平台或大型企业客服来电,应提高警觉



真实案例（部分情节经过改动）

为取消外卖损失4,300元

「你的订单#12345已确认,扣款1,200元,如有疑问请致电12345678。」

家庭主妇李小依(化名)拿起手机一看,大惊,心想:吃什么外卖要花1,200元,自己明明没有叫外卖,怎会有订单?难道是丈夫的?抑或是外卖App出错?完全没理由呀……

为了取消这扣款,小依回拨短讯内的电话号码找客服。

- 小依:我收到你们的短讯,说我下了1,200元订单,还已经扣钱,我根本没有订过!
- 客服:你好!请问小姐你怎样称呼?请提供订单编号。
- 小依:12345。我姓李。
- 客服:感谢李小姐,我这里查到你的订单已获确认,订餐餐厅是中环XYZ饭店,你确定没有下单吗?
- 小依:没有,你们肯定出错,马上帮我取消扣款。
- 客服:一般而言,我们不可以取消客人已确认的订单,但在这特别情况下,我可以帮你申请取消,需要三个工作天处理,请提交4,300元保证金。
- 小依:为什么要付保证金?还那么多?
- 客服:噢!那只是程序上需要,如果调查结果显示是我们出错,会退还所有款项,请放心。
- 小依:唉,那好吧!怎样交?

于是,小依按客服指示,汇款4,300元到指定银行账户。

结局:

小依其后登入外卖App,却发现没有这张订单,短讯发送人名称也不像平日般带有「#」号。小依在App内联系真正的客服,才知道自己受骗。



02

假冒身份篇

假冒客服

特征

发送人名称没有以「#」号开头

可疑连结 官方App无相关通告

要求共享手机画面

要求输入网上理财密码

防骗技巧

- 慎防没有以「#」号开头的短讯发送人名称
- 别回拨短讯中的电话或点击连结
- 致电相关机构热线核实，而非短讯中的电话

认清!

认清「#」号

慎防！



客服

假客服·借口·付款

= 骗钱

假冒

遇到有人自称
支付平台或大型企业
客服来电
应提高警觉



香港短讯发送人名称以「#」号开头，表示短讯由经官方认证的机构发送。以「#」开头标示登记名称，作用是防止假冒、反诈骗及提升短讯可信度。

目前，短讯发送人登记制已涵盖政府各部门、主要银行、电讯商等各行各业。

名册可到通讯事务管理局办公室网站查核。

迷失「#」

HSBC

今日下午 2:55

【汇丰银行】经本人授权体验腾讯保险将于今日从本行户口扣除 25920 HKD，保单已生效详情洽保险官网 <https://iobuor.xyz>

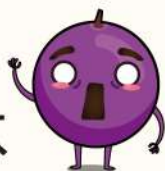
HOY TV

Text Message - SMS
Today 11:39AM

您已成功续订Netflix家庭版会员服务，月费HK \$2180.00若非您本人操作，请您联系客服取消：30016134



股市神童 在社交媒体



教你投资?

手法

1. 骗徒利用官员或名人的图片或录音，窜改公开片段



诱骗事主投资

2. 骗徒从社交媒体、视讯通话或网上的公开影片取得他人的面容，声音等生物辨识资料



通过深度伪造(Deepfake)技术假冒

你的亲友



骗取事主金钱及个人资料



如何辨别影片是利用人工智能(AI)制成?

面部表情不自然	光影效果异常	声音与口型不匹配
边缘模糊或变形	背景不稳定	过于完美而显得不真实

防骗技巧

进行视讯聊天时，如何确认对方是真人?

要求对方作出随机动作

(例如：用手遮住左眼/举起三只手指)

检查声画是否同步

观察嘴唇动作与声音是否一致



AI换脸骗案

真实案例（部分情节经过改动）

公司「会议」出席者全是Deepfake产物

在一场公司高层视讯「会议」上，贾琛（化名）单独代表香港分公司出席，他神色凝重，表情紧张。

这是因为他先前收到一封来自海外总公司「财务长」的秘密电邮，「财务长」在电邮告诉贾琛，公司正进行一宗「秘密大额交易」，需要动用香港分公司的资金。贾琛认真细看电邮的用字，的确和财务长写的一样。

电邮里附有一个视讯「会议」连结，写着今日下午二时会有一场高层「会议」，多地分公司都会派「代表」出席。

视讯「会议」接通后，贾琛看到很多熟悉的脸孔，也听到很多熟悉的声音，包括总公司的「财务长」和多地分公司的「代表」。「财务长」认真地就电邮里谈到的「秘密交易」向各人作指示。

经过这场视讯「会议」，按「财务长」的指示把总额两亿港元的资金汇到多个指定银行账户。

结局：

贾琛汇款后在一个会议上查询时，才揭发这是一宗AI换脸骗案。该视讯「会议」的出席者除了贾琛外，全是骗徒利用Deepfake深伪技术伪造。

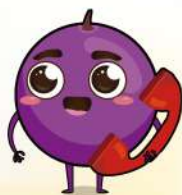




亲戚突然来电

向你

借钱?



手法

1. 打电话与你闲话家常



但不会说出自己是谁

诱导你猜测身份，对方马上冒认

2. 在 WhatsApp 使用 AI 合成声线扮作你上司、亲戚等身边人



用各种藉口借钱应急

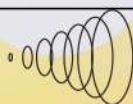
例子: 被捕急需保释金 / 代公司垫支转账



防骗技巧

- 直接询问对方姓甚名谁
- 试探对方身份是否真确，并可致电其他亲友确认
- 遇到借钱或紧急求助，务必冷静求证





真实案例 (部分情节经过改动)

扮老友论点心

电话响起……

- ▲ 何仁(化名):喂,是哪位?
- 来电者:喂,好久没见,你认不出我吗?
- ▲ 何仁:我还真认不出,你是?
- 来电者:你可真会说笑,早阵子我们一起吃过饭。对了,吃饭没有?
- ▲ 何仁:还没,正准备去楼下喝茶呢!
- 来电者:你楼下那家不好吃,下次和我一起去湾仔水鱼茶楼,那里的烧卖可好吃了。
- ▲ 何仁:那家是挺不错。我跟你去过那家吃吗?
- 来电者:我就说嘛。那家是很不错。除了烧卖,还有虾饺、珍珠鸡都还可以。
- ▲ 何仁:对对对,都还可以。啊……我想起来了,你是不是老陈的那个朋友?
- 来电者:不就是我吗!你再不说,还以为你真认不出来。
- ▲ 何仁:哈哈,老了,记性差多了。怎么你换了电话号码?弄得我以为是诈骗。
- 来电者:我最近换了电话号码,你就认着这个号码好了。
对了,老陈的事你听说了吗?
- ▲ 何仁:老陈他怎么了?
- 来电者:他最近生意周转不灵,你没听说吗?
- ▲ 何仁:他不是帮人打工吗?怎么会有生意。
- 来电者:噢,他没跟很多人说,他跟朋友合资做小生意,怎料那个朋友因为欠债跑路了,现在差12万元才可以做下去。我跟其他人已经凑了8万元帮一下老陈,你看看要不要也帮他一把。
- ▲ 何仁:他老是被当水鱼,也不是第一次了。
- 来电者:其实他那门小生意还可以的,就是缺了资金周转。
- ▲ 何仁:唉……好吧,老陈也肯定不好意思问人拿钱,算上我,我出4万元吧。
- 来电者:都说你是老陈最好的兄弟,那你转账到水鱼银行,账号是123123456789。由我统一计算,再转给他。



结局:

过了一段时间,何仁相约老陈吃饭,问起借钱一事,对方却说不知情,亦否认与他人合作做小生意。两人拨打所谓「老陈朋友」的电话已无人接听,惊觉被骗,遂到警署报案。



05

假冒身份篇

假冒技术支持骗案



在网上网时电脑 突然弹出警告视窗?

手法

你浏览网站时，画面突然弹出视窗，显示电脑中毒警告，附有求助电话号码，诱骗你致电求助



骗徒假扮电脑技术支持人员接听电话，要求你下载远端操控程式，并开放电脑权限



遥距控制你的电脑，声称发现违法行为，转介至假冒警察的骗徒



讹称要追踪黑客，指示你在电脑输入密码，检查银行账户



骗徒进行「检查」时，同时窃取银行理财密码等个人资料，最后转走存款





真实案例（部分情节经过改动）

「细心客服」引导入局



退休人士姚小心（化名）在社交平台收到一个好友邀请通知。仔细看过对方的简介后，他同意了这个好友邀请，谁不知一按下去电脑突然出现当机画面，并出现了Microsoft Defender的警告：

“你的电脑可能正遭受病毒攻击，请不要作出任何动作，并致电Microsoft团队以解除封锁。电话：12345678。”
Microsoft 团队

小心本来打算重新开机，但又看见警告视窗出自Microsoft这家大型软件公司，想一想觉得还是打电话寻求帮助更好。

接通电话后，小心听见一把操印度口音的英语声线，对方介绍自己为Tom Jones，是「Microsoft」的「客户技术支持专员」。他仔细聆听姚小心形容的当机画面，详细地向小心说明电脑问题所在。小心对其态度非常满意，按他建议下载了远端操控程式，开放权限方便让他详细检查电脑，两人不知不觉聊了近两小时。

忽然，Tom Jones通过聊天软件发送截图给小心，表示发现其电脑被黑客入侵，指示小心填写表格，并指会马上转介至香港警方跟进。

小心此时已经有点迷失，只想尽快解锁电脑，急急填妥表格并发送至指定电邮。果真，他很快便收到电邮回覆，详列了他的个人资料、案件编号，以及负责调查警员「黄警官」的联络资料。

不久后，有一个视讯电话打进来。接通后，一位身穿警服的男人笔直坐着，自称是「黄警官」，表示小心的电脑涉及国际洗黑钱罪行，指示她在电脑输入银行资料，说着电脑便自动跳出银行登入介面。小心心想这次有大麻烦了，马上按指示输入……

结局：

骗徒短时间内便把约500万元的存款转走，小心察觉不对劲，前往警署报案，但为时已晚。



05

假冒身份篇

假冒技术支持骗案—◆ IIII

特征

不明来历警告视窗 声称「账户遭入侵」

声称「问题严重」、「账户将被冻结」

要求授予远端操控权

要求你致电客户服务人员

防骗技巧

- 按 **CRTL** + **ATL** + **DEL**

开启工作管理员，重新启动电脑即可

- **切勿随意下载远端控制程式**，
或将电脑远端操控权授予陌生人
- 不要拨打警告视窗的电话号码





网上交易篇

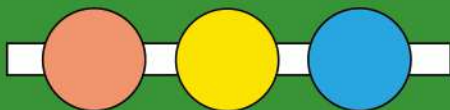
SCAM ALERTS

SCAM



社交媒体

出现异常便宜的租盘?



手法

租客扮作业主转租物业 /
「假业主」在社交媒体出租假物业



租金异常便宜，甚至使用假相片
吸引你



诱骗预付全年租金



租屋陷阱



SCAM ALERTS

SCAM ALERTS

SCAM ALERTS

租屋骗案



真实案例（部分情节经过改动）

「高质楼盘」的真相

内地生萧虹舒（化名）喜获奖学金来港读书，她兴奋到马上在小红书寻找租房资讯，看到一家「中介公司」的出租单位，月租2万元，罕有350呎的大空间，邻近学校，还有会所，适合学生租客。

虹舒检查了一下「中介公司」的小红书账号，发现该「中介公司」不单盘源多，单位质素都很高，同时影片也显示有实体店面，心里想「心动不如行动」，马上询问详情。

★ 中介：你好！感谢查询，这个单位月租18,000元，按香港法规，租户需要交两按一上（两个月按金、一个月上期），如果能以现金一次过缴交一年租金，更可享八折优惠，要不要考虑一下？

● 虹舒：那就是一次过交226,800元？不用佣金吗？

★ 中介：对，佣金全免，还省了四万多，这价格绝对划算，现在开始旺季了，再晚就可能要租出。

虹舒问了一下父母的意见，他们都倾向一次过交一年租金，让女儿安稳在港读书。因怕被其他人租用，所以在没有先来港看房下，虹舒便将一年租金缴交予「中介公司」。

到了开学季，虹舒一个人带着两个大行李箱，提前来港，准备到「中介公司」取锁匙入住上述单位，才发现该「中介公司」并不存在，惊慌失措的她唯有报警寻求协助。

结局：

警方调查发现涉案「中介公司」并非持牌地产代理，真正的业主也没有经该「中介公司」放盘，骗徒只是借其照片骗取租金。虹舒为了继续学业，只好再花一笔钱租房。





▶ SCAM ALERTS



SCAM ALERTS



SCAM ALERTS



SCAM ALERTS



SCAM ALERTS



SCAM ALERTS



防骗技巧

- 签署租约时，要留意文件是否正规租约，以及出租人是否真正业主
- 应直接联络持牌地产代理，并实地视察物业后再考虑是否租用
- 可向地产代理营业员查询其全名及牌照号码，并到地产代理监管局网页核实对方是否持牌



骗上骗

租上租



成功入住也被骗？



有受害人通过所谓「中介公司」预付了一年租金，入住了三个月，但其后发现「中介公司」实为二房东，仅仅租下单位三个月，然后「租上租」予受害人，而且收到的租金也没有交予业主。

▶ SCAM ALERTS



SCAM ALERTS



SCAM ALERTS





机构发短讯



要求你 填资料?

手法



黑客假冒银行、电讯公司或任何机构设置钓鱼网站
外表跟真网站几乎相同



黑客向大众发放钓鱼电邮或短讯
行文及格式都和上述机构发放的信息 非常相似



引诱受害人点击假连结，修正「异常情况」



假连结转驳到钓鱼网站
在受害人输入个人、信用卡或
网上银行资料后，骗徒便转走存款





●●● 真实案例（部分情节经过改动）

一条短讯投资清零

金融分析师John热衷投资美股。某日，美股开盘飙升，John全神贯注为客户整理数据。这时候，手机收到一条看似来自他惯用的投资平台的短讯：



John因太忙，未及细想下点击连结，网站与他熟悉的投资平台界面无异。他熟练地输入账号、密码和验证码，登入后，页面迅速跳转至填表界面。John匆匆填完以便尽快「解除冻结」，继续埋首工作。

他浑然不觉，自己的投资账户已悄然落入黑客之手，投资平台App通知功能被暗中关闭，股票已被全数卖出也没发现。

一日后，John打开投资平台App查看投资组合表现时瞬间惊呆——他精心买入的优质美股荡然无存，账户仅剩一堆陌生的冷门股票和衍生产品。他怀疑登入错误，反覆核对账号密码，终于确信这正是自己的账户。

结局：

John账面亏损高达250万元，及后马上为账户设置多重验证功能，以策安全。



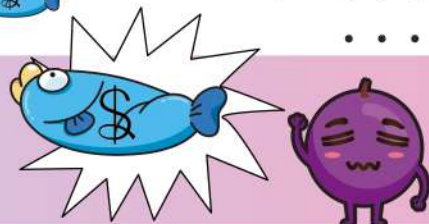
07

网上交易篇

钓鱼 骗案

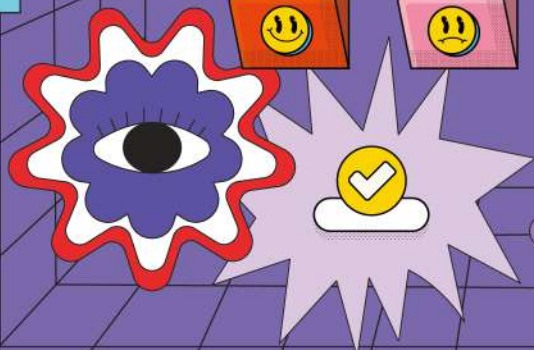


防骗技巧



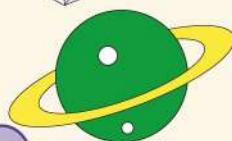
- **直接联络** 相关机构确认电邮或短讯是否真实
- **切勿点击** 可疑电邮或短讯内的连结
- 提防 **没有以「#」号** 开头的短讯发送人名称

CLICK





网上 广告推销 大额折扣优惠?



手法



骗徒假扮卖家

在社交媒体或买卖网站发贴文或开设
 专区,以优惠价、限购等字眼吸引注意



要求买家先付款后收货,更只接受以
 转账、转数快或储值支付工具付款



在收到款项后失去联络



骗徒假扮买家

一: 联络卖家,声称大量购货 /
 愿意以高价买入货品



发出虚假收据-以虚假入数收据作转账证明



发出无效支票-将未能兑现的支票存入卖家
 户口,制造虚假入账记录



在收货后失去联络



二: 假扮已经付款-发连结要求你输入银行
 资料及一次性密码,然后转走你的存款

网购骗案

真实案例 (部分情节经过改动)

假期机票买一送一

SHOP NOW

距离复活节还有一个月,汪少飞(化名)的同事在聊假期到哪里旅行,有的会北上、有的打算去欧洲,他自己没有任何计划。

回到家里,少飞拖著工作疲惫的身躯,瘫软在沙发上,手指头机械地滑著手机屏幕。隔了一会,一个广告吸引了少飞的目光:

【限时优惠先到先得】往来日本香港机票买一送一 复活节假日可用

WhatsApp电话号码: 12345678

少飞再往下看,广告帖文只发布了数小时,但已经有几十个点赞和留言。他马上打电话给女朋友吴小姐。

少飞: 宝贝~复活节想不想一起旅行?

吴小姐: 好呀,我也想去日本逛逛!

少飞: 正好,我刚在Facebook看到有机票买一送一优惠。

吴小姐: 你这个小傻瓜,没看ADCC网页吗?不少人网上买机票都被骗,先看一下那个广告帖文的作者资料吧!

少飞: 噢,这个作者的账号昨天才建立的,真的是骗子!

结局:

有女朋友提点的少飞察觉出是骗局,两人其后改用正规渠道买机票,旅程顺利。

SHOP NOW

Buy
get 1

BIG DISCOUNT

机票买一送一

SALE

特征

超低价格

私下交易

催促付款

假物流单号

假平台或网站

无联络方法

防骗技巧

- 银行账户的「**可用结余**」才是反映账户内可供提取的款项
- 留意网店注册日期、交易评价及**信誉评级**
- 以**当面交收**或**货到付款**方式交易，避免通过不明连结交易

SHOP-
PING
DAY

租/借/卖银行账户—◆

借出银行账户

可以赚钱？

提
提
你！洗黑钱是刑事罪行，最高刑罚为罚款
港币5百万元及监禁14年

手 法



- ① 虚拟交易 - 声称作**加密货币交易**用途并提供报酬
- ② 求职陷阱 - 标榜「**赚快钱**」，诱使求职者提供银行账户
- ③ 明买明卖 - 利诱出租或卖银行账户，标榜「**安全不犯法**」
- ④ 网上情缘 - 利用交友 App 与你发展**网上情侣关系**，取得信任后要求协助开户

骗徒利用银行账户作傀儡户口，以**清洗黑钱**

切勿贪心

以免堕入圈套

被不法分子利用



8,000元的诱惑

17岁的伍浩信(化名)已不能登入网上银行账户,一边盯著手上的一叠钞票,一边陷入了沉思。

一周前……

浩信被同学邀请去唱卡拉OK,但因已花光零用钱,所以借口说有事不去了。一名死党看出了他的心思,在他耳边说:「放心,有大哥请客。」

到了卡拉OK店,浩信发现有几个不认识的人,一身潮流名牌,死党介绍说这几位都是做兼职认识的同事,都很会赚钱。一群人唱着唱着很快就熟络起来,而浩信也耐不住好奇心……

- 浩信:你做什么兼职呀?为什么你的同事看起来都那么有钱?
- 死党:其实都算不上工作,他们只是借我的银行账户去炒币,定期给我一笔出租费。
- 浩信:多少钱呀?
- 死党:8,000元。
- 浩信:哇!这么多,合法的吗?
- 死党:当然合法,都不知道多少人炒币致富了,而且他们比你更注重资金安全,存一大笔钱在你账户之前,都要求你先提交身份和住址证明。
- 浩信:我也想加入,可以帮我介绍吗?
- 死党:这……好吧,我帮你问一问。

结局:

浩信以8,000元出租银行账户,一年后被警方拘捕,因为其账户被查出涉及清洗500万元犯罪得益,区域法院经审讯后裁定他罪名成立,判囚42个月。



10

情感利诱篇

裸聊骗案



交友App

新相识要你

下载程式?

结识受害人 ♥ 聊天建立信任

手法

通过社交媒体、交友App或即时通讯软件结识你，藉聊天建立信任



引诱你进行裸聊及**下载恶意程式**，以盗取通讯录资料



拍下裸聊片段，**威胁传至你的亲友**，并要求汇款到指定账户，或以加密货币或点数卡支付款项

防骗技巧

- **切勿** 在进行视讯聊天期间裸露身体
- **切勿** 点击不明来历的连结或下载程式
- **切勿** 轻信对方是以「真面目」示人

裸聊骗案

真实案例（部分情节经过改动）

可爱女孩瞬间变脸

17岁的林一夏（化名）刚刚失恋，某天晚上在网上交友平台寻觅聊天对象时，匹配到了一位叫「小雅」的文青女孩。她的头像是一张清纯的笑脸，自我介绍写着「喜欢看电影，寻找有共鸣的灵魂」。

聊天记录

- ★ 小雅：Hi，好久没遇到香港男生了，你平时喜欢做什么呀？
- ♥ 一夏：Hello！我平时就看看Netflix，偶尔打打游戏。你呢？
- ★ 小雅：我超爱看电影！最近在追一部悬疑剧，紧张得我晚上都不敢一个人睡，你喜欢什么类型的电影？
- ♥ 一夏：悬疑片我也喜欢！最近看了《消失的她》，觉得还不错。你有推荐吗？

两人话题慢慢从电影扩展到生活，轻松又愉快。聊到第三天，小雅突然提议视讯聊天，并发来一个连结，说是一个平台的私人房间，保证私隐有保障。一夏点击进去，小雅出现在荧幕上，样子跟头像差不多，完全没有「照骗」。

- ★ 小雅：哈哈，看到你了！好帅哦！要不要放松一点，我们玩点刺激的？
- ♥ 一夏：刺激？什么意思？
- ★ 小雅：嘻嘻，比如……我们玩个游戏，谁输了就脱一件衣服，敢不敢？

那天晚上，两人聊了快一个小时，画面越来越大胆。视讯突然中断，小雅发来一段三分鐘的影片，竟然就是刚刚裸聊的画面！

- ★ 小雅：不要生气！小妹想赚点生活费，转5,000元给我就把影片删了，要不然我就把影片传给你的朋友、家人，并上载到互联网。

一夏整个人愣住了，心脏狂跳，尝试问小雅为什么要诈骗他，是不是受人威胁等。小雅没有回应，只是再度要求他转账。焦急的一夏把自己的零用钱都转账给他了。正当以为事情可以告一段落，小雅再以「删除手续费」为由，要他再转2万元，并不断用言语威胁他……

结局：

一夏偷用父母手机在网上银行转账时被父母发现，再三询问之下，一夏向父母坦承错误，马上到警署报案求助，除了一开始的5,000元外，没有更多损失。

11

情感利诱篇



网上投资骗案——

突然被拉入WhatsApp
投资群组？

手法

骗徒通过社交媒体宣传，声称有内幕消息，假扮专家教投资或随机拉拢市民加入WhatsApp「投资教学」群组



伪造交易获利记录，在群组分享「获利截图」，游说安装虚假投资平台App



骗徒伪装成客服人员，要求你提交个人资料及转账至指定银行账户



初期给予你小额回报，目的是吸引你加大投资额

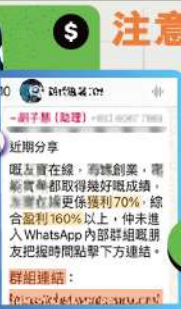


你欲提取资金时，客服人员用各种藉口拖延付款，甚至要求支付大额手续费；最终你无法取回任何资金



认清 NOTICE

注意 诈骗讯息叫你投资



情感利诱篇

网上投资骗案

「投资名人」贴身教学

余青凌(化名)是中学教师,存了可观的积蓄,最近股市复炽,加上看了许多投资专家的YouTube影片,因而一直留意有没有投资良机。

某日,她被陌生人拉进一个WhatsApp群组,名为「流大师AI投资教学谷」,群组内有多达180人。她被拉进去时,群组成员已经聊过不停,所有人都称赞大师的预测专业,还有人贴出截图,说自己每一天都赚7%。

「一天7%,才不信呢!」青凌心想这肯定是诈骗群组,不过她抱着好奇心没有删掉群组,默默地观察。隔天,群组管理员流大师的发言改变了她的想法……

- 大师: 各位投资界朋友,小弟已经连续两周成功预测每天会升7%以上的股票,你们肯定好奇我是怎样做到?其实不是小弟厉害,现在股票预测已经是电脑超越人脑的时代了。我所用的是最新人工智能,它能批量分析每天的金融市场消息,看出人类难以理解的细节,从而准确预测股票走向。大家要记住股票市场其实就是一场心理学博弈,AI既能吸收大量资讯,又能理性分析这些资讯,必定更胜一筹。
- 群组成员A: 感谢大师分享,那AI投资会有风险吗?
- 大师: 任何投资都有风险,关键在于使用AI能大大把风险降低。
- ★ 群组成员B: 大师推荐什么投资平台?
- 大师: 市面上很多流通的投资工具没有AI功能,所以我个人推荐使用这个「AI猫猫投资平台」。

青凌对流大师改观,觉得他不像其他投资专家一样,一味吹捧自己,甚至很尽力教育成员AI投资的好与坏。青凌还发现原来流大师曾经上过电视财经节目,是响当当的投资专家。

不久后,群组管理员私信青凌,问她有没有兴趣加入「流大师粉丝专属贴士群」,并说流大师会提供在AI猫猫投资平台投资的专业意见。青凌感觉可以小试牛刀,便按连结指示下载投资App和注资10万元。

果真,青凌隔两天赚了三万多元。其后再充值,愈充愈多……

结局:

青凌眼看已经赚了三千多万元便想提款,怎料遭客服拒绝,更被要求提交500万元保证金,青凌拒绝,自此无法登入该App,遂报警求助,终于醒觉是骗徒冒充投资界名人混水摸鱼。



11

情感利诱篇

特征

高回报低风险承诺

平台无注册或认证

无法提款

不断诱导追加资金

盈利短期大幅上涨



防骗技巧

- 到**证券及期货事务监察委员会网站**查证投资平台的背景及注册信息：

https://sc.sfc.hk/TuniS/www.sfc.hk/TC/Alert_List

- 作大额投资前先谘询专业人士（例如律师或金融顾问）
- 避免通过社交媒体或陌生网站寻觅投资机会



认清楚

天上不会掉馅饼

注意白撞信息叫你投资





向对象快速

发动追求攻势?



用「高富帅」、「白富美」或「专业人士」

的相片做头像，在社交媒体或交友App寻找目标



发动追求攻势，建立网上恋人关系

然后用各种借口骗财

例子：

- 突然急需缴付巨额医疗费
- 寄出的贵重礼物被扣查，需要清关费
- 答应见面，但要求垫支行程费用
(例如：机票费用)



真实案例（部分情节经过改动）

忘年的漏水情缘

「你好，我姓王的，刚搬来你楼下住，发现天花板有点漏水，所以从管理处取得你的电话并联络你，希望能和你商量一下。」林近麟（化名）退休多年，收到这则短讯后甚是疑惑，原因是自己和楼下邻居陈先生一家认识多年，没听过他们要搬走。

「你是陈先生的租客吗？」问毕，对方沉默良久。

「噢，看来我搞错电话号码了，我刚从新加坡来香港工作，要办的事情太多了，人生路不熟，忙中有错，对不起了，打扰了这位大哥。」这番话让近麟想起当年自己也是只身来港，经历各种风吹雨打才有了现在的生活。

「绝无打扰，小事一宗，王小姐一个人来香港辛苦了。小姓林，既然有缘，王小姐如在香港遇到什么难题，不妨与我分享解忧。」

「谢谢你，林大哥，我叫王薰，你是我来香港遇上的第一个好人。」

光阴似箭，一个月过去了，两人没有因年龄差异而有隔阂，感情发展飞快。近麟尤其欣赏王薰坚强独立。而王薰也对林大哥打开心窗，互生情愫，在某一次欢快的聊天中承认了这段忘年恋。

「你明知我对你动了情……要听话，好好珍惜我。」

又过了一个月，两人偶尔聊到投资，发现大家想法有很大分别。

 近麟：股神巴巴特也说宁愿买砖头，都不买比比币。

 王薰：林大哥，他这么说证明他太老派了，现在一枚比比币都值好几间房子了。

 近麟：真的吗？

 王薰：你不信我吗？我在交易所工作，对这些最清楚了。我发你一则新闻，你看看就懂了。如果我现在有一笔钱，肯定会投资比比币，这样以后就可以整天陪你，不用工作了。」

该则新闻报道，加密货币近年价值倍增，已造就许多人一夜暴富，近麟慢慢认同王薰的想法，更在她的指导下用退休金学习投资加密货币。

结局：

近麟多次转账至不同的银行账户，而银行职员发现其中一个账户有可疑，随即通知反诈骗协调中心揭发骗局。至此，近麟已被骗约320万元。



特征

完美人设

拒绝亲身见面

快速建立亲密关系

拒绝视讯通话

情绪勒索

突然急需金钱



ROMANCE SCAM



防骗技巧



- 要求与对方进行 **视讯通话**
- 利用 **搜寻器** 查看对方相片确认来源
- 通过不同方法 (社交媒体、视讯通话) 查证身份，留意言行是否一致



「刷单赚佣」求职骗案—

WhatsApp 群组教你

做任务赚钱?

手法



在社交媒体刊登广告 招聘「点赞员」或「下单员」



声称只需以购物刺激销量便能抽佣赚钱



要求你先垫支购物款项
并将款项存入指定银行账户

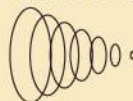


在交易初期，骗徒或发放少许佣金，令人信以
为真，再指示垫支更多金钱，最后失去联络

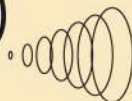




情感利诱篇



「刷单赚佣」求职骗案



找一份兼职竟被骗二次

市道不景气，薛清江（化名）最近在网上留意有没有兼职适合自己。清江原本只想找周末侍应的空缺，但一个广告吸引了他的目光：

你是否厌倦了朝九晚五的工作？

我们来自大型购物平台XYZ Mall，现诚聘以下职位：

刷单员

- 日薪1,000至2,000元
- 无需经验，在家工作，只需操作手机
- 专业培训，只要你肯学，保证教你上手

有兴趣请加WhatsApp: 12345678



清江没试过在家工作，不过自认勤奋好学，觉得既然有培训，那就可以一试。于是，清江经WhatsApp加入了一个二百多人的聊天群组。

群组管理员介绍称，刷单员的职责是帮公司下单购买电器，制造更多单数，让产品看起来更受欢迎，完成后公司会立即退回本金和10%佣金，也就是说买的货品愈贵，回佣愈多。清江看见群组成员不停分享赚钱截图，又有热心成员私下发讯息游说，便用数十元买小电器试试，很快就获得全额退款和二十多元佣金。

清江态度瞬间积极起来，不停参加刷单任务，购买总值超过20万元的电器，却换来群组管理员指责「操作不当，拒绝退款」。清江气得报警，证实是遭到诈骗。

三周后，清江仍为此愤愤不平，偶尔在社交媒体上看到一个律师广告，「专业地为被骗人士追讨赔偿，不成功不收费」，清江二话不说，马上联络「律师」。

不久后，「律师」亲自致电清江，指自己追踪到骗款被汇到澳门一间赌场，现在清江需要立即交20万元保证金予赌场以冻结骗款，否则赌场不会帮助他，款项再追查不了。

结局：

清江情急之下再付20万元积蓄予假扮律师的骗子，惨遭二次诈骗，花光了积蓄才报警求助。

13

「刷单赚佣」求职骗案

情感利诱篇

特征

经验及学历不拘

以简单任务开始

只用社交媒体账户联络

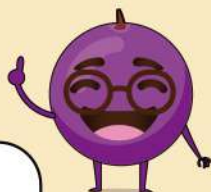
拒绝发还本金

要求先垫支款项

失去联络

防骗技巧

- 不要相信声称职位不拘学历或经验，但可享高薪的招聘广告
- 通过可**信赖的求职途径**求职
- 应聘前先了解**公司背景及业务性质**



骗人招聘



认清 NOTICE

刷单任务 = 破产之路

1. 陌生

群组名称含有大型机构名字

2. 虚构

专业客服人员名称

3. 假扮

客服系统自动回覆

3 伎俩令你松懈

WhatsApp 陌生信息



14

情感利诱篇

网上求职骗案(人口贩卖) —

东南亚公司 请你出任



高薪厚职?



JOB 苟工
HUNTING



骗徒在社交媒体或娱乐场所寻找目标



邀请你到外地工作·标榜「**东南亚高薪厚职工作**」

「无需学历或工作经验」「包机票食宿」



抵达后被没收护照及手机



被不法集团贩卖到诈骗园区从事诈骗工作
可能受到身体虐待甚至失去性命



恐怖免费旅行

年轻貌美的宋小珠是「月光族」,有钱就花,没有积蓄,闲时喜爱到酒吧里喝喝酒聊聊天。某日,她在酒吧通过朋友认识了一个大自己几年、姓郭的女人,对方一来就请她喝酒,挥金如土,像极富家大小姐。

小珠想着有「免费午餐」那么好,就多次主动上前示好,又不停敬酒给郭小姐,说好话,哄得她非常开心。郭小姐在酒局后带着酒劲抱小珠,念念有词地说想继续喝,不想离开小珠身边,甚至说要请小珠明天一起去旅行。

起初,小珠以为郭小姐只是开玩笑,岂料下一秒她真的问小珠拿身份资料,用手机买机票。小珠顿时不知如何是好,想劝阻郭小姐,却被她一手挡开,说「你明天拿行李来机场就好,我会照顾好你。」

第二天,小珠半信半疑地拖着行李到机场,竟然真的看到郭小姐笑着走来,说要带她离开香港好好放松,「别想那些鬼东西了,人生太短,要努力让自己开心,我以后叫你妹妹,好不好?」,小珠开心地笑了。

下机后,小珠跟着郭小姐走,突然两个男人走来强行抓住她,抢走她的护照及手机后把她抱起带上一辆私家车。小珠一路挣扎大叫,附近却奇怪没有什么人,郭小姐转眼也不见了。

结局:

小珠被送到诈骗园区从事诈骗工作,幸未曾受到虐待,最后获释。警方以串谋诈骗罪拘捕郭小姐,原来其职业是美容师,为了赚钱参与人口贩卖,四处寻找猎物。



特 征

高度
风险

高薪厚职

职责说明模糊

没收护照

限制自由

快速录取

包机票食宿

防骗技巧

- **切勿轻信**「高薪厚职」、「无需学历或工作经验」、「包机票食宿」等「赚快钱」的机会

- 与亲友 **保持联系**，告知具体地点及行程

- 入境事务处「协助在外香港居民小组」

24小时求助电话：
+852-1868

- 微信求助：关注「香港入境事务处」官方账号，然后按「**1868求助热线**」联络小组

核实公司资料

快逃!

快逃!

哪里有这么好



「骗案预警」计划

反诈骗协调中心联同银行持续监测可疑交易与银行账户，一旦市民转账至可疑银行账户，「防骗预警」便会启动，由银行职员或警方告诫市民停止可疑交易。

我们会向潜在受害人：

发出警示短讯 | 派警员上门提醒 | 致电作警示
在这个时候，你应该立即停止可疑转账或交易，并提高警惕。



「骗案预警」计划

反诈骗警示及建议会以下列途径发放：



或



或



提防骗徒假冒「反诈骗协调中心」

1. 中心的短讯发送人名称为「#ADCC18222」，短讯并不会附有任何连结
2. 中心不会指示受害人转账及要求提供银行理财密码
3. 如对中心人员身份存疑，可致电

18222 热线查询

警方亦推出了「防骗视伏App」流动應用程式
协助市民辨识诈骗及网路陷阱和提升他们的防罪意识



关注我们

香港警务处电子报案中心

<https://crp.police.gov.hk/crp001?lang=sc>

「防骗易18222」热线

怀疑受骗
即打 **18222**
www.adcc.gov.hk

「防骗易18222」二十四小时电话咨询热线，为市民提供即时谘询，以便更有效处理怀疑骗案

「反诈骗协调中心」网页

<https://www.adcc.gov.hk/zh-cn/home.html>

关注我们获取最新防骗信息

Website



小红书



TikTok



YouTube



下载及安装「防骗视伏App」应用程式

<https://cyberdefender.hk/zh-cn/scameter/>

协助公众辨识诈骗及网络陷阱，透过输入有可疑的平台账户名称、银行账户号码、电话号码、电邮地址等，以评估诈骗及网络安全风险



「守网者」一站式网络资讯平台

<https://cyberdefender.hk/zh-cn/>

立即获取最新网络安全及防骗信息

Youtube



Facebook



Website



Instagram

