假冒库务署短讯出现 附连结要求缴交罚款

手法

骗徒假冒库务署，发出钓鱼短讯，要求收件人点击短讯内的超链接以缴付定额罚款。库务署强调，署方与该短讯无任何关系，并提醒市民，署方不会向市民发出附有超链接的短讯并要求缴款。

警方呼吁

切勿随意点击可疑短讯、电邮或网页内的超链接，以进入任何网站或下载附件；

切勿在不明来历的应用程序或网站输入个人、信用卡数据、三位数安全码(CVC/CVV)及一次性密码；

除了向指定机构验证，市民也可在守网者网站「防骗视伏器」或「防骗视伏App」手机应用程序输入可疑网址，以作查核；

提醒身边亲友慎防受骗；

如有怀疑，可致电「防骗易18222」热线查询。

「告票电子化」防骗须知 记得要睇有无「#」号开首！

警惕钓鱼短讯

警方将于6月中旬试行交通违例告票电子化，以手机短讯（SMS）或电子邮件发出告票。届时，警方会推出电子交通执法专属网站及流动电话应用程序，让车主及司机核实及查阅电子通知书，并以电子途径例如网上信用卡及「转数快」系统等，于网上清缴罚款。

为提防钓鱼短讯出现，请市民留意以下防骗须知：

1. 「短讯发送人登记制」——「#」

警方已登记参与通讯事务管理局办公室的「短讯发送人登记制」，所以，将来的短讯告票会使用以「#」号开头的；「已登记的短讯发送人名称」——「#HKPF-eTT」。

2. 不会附有任何超链接

不论是短讯告票或者电邮告票，都不会附有任何超链接。

3. 网址域名——「.gov.hk」

警方的「电子交通告票平台」（www.etraffic ticket.gov.hk），如同其他香港政府官方网站一样，网址域名结尾均必定为.gov.hk。例如：警务处的官方网站www.police.gov.hk；或运输署的官方网站www.td.gov.hk。

注意：

1. 切勿随意点击任何电邮或短讯内的超链接。
2. 于未确定对方身份前，切勿透露任何个人或账户资料。
3. 如有怀疑，请即打防骗易热线18222与警务处反诈骗协调中心联络。

提防假冒警务人员电话骗案

手法

最近，有骗徒假冒香港警务处高层人员，以电话号码+852 5687 4117 向市民发送 WhatsApp 讯息，讹称市民曾经参与非法活动，要求市民转账至指定加密货币户口作「放行费」，以协助调查。过程中，骗徒盗取警务处高层人员照片作 WhatsApp 个人头像，藉此取得市民的信任。

警方呼吁

- 即使发送讯息的陌生人能说出你的个人资料，并不代表他是真正的执法人员，因为骗徒可以通过非法手段取得市民的个人资料；
- 真正的执法人员调查案件时，并不会索取你的网上理财密码或指示你将钱转账到指定银行账户；
- 如遇到有人自称执法人员或政府机构职员，以不同理由指示你交出个人资料及财产，你应该主动查证及再三向相关机构核实对方身分；
- 如有怀疑，可致电「防骗易 18222」热线查询。

提防假冒「HKTVmall」刷单赚佣骗案

手法

近日，有骗徒假冒HKTVmall 随机将市民新增至 WhatsApp 群组。部分骗徒声称市民只要收藏产品，再以截图作证明就可以获取酬劳。该等骗徒会要求受害人浏览伪冒钓鱼网站或下载假应用程序，然后作登记，以骗取受害人的个人资料。亦有骗徒要求市民垫支刷单，在 HKTVmall 将货品放入购物车后传送截图予骗徒，再指示受害人将货款存入指定个人账户。初时，骗徒会兑现承诺，将货款及佣金汇给受害人，令受害人信以为真。因此，受害人垫支更多金钱，以作更大额的购物，但骗徒在取得款项后已逃之夭夭。

保障自己

市民可在 WhatsApp「设定」>「私隐」>「群组」的「谁可将我新增至群组」列表中，选择「我的联络人」，避免被陌生人新增至群组。

警方呼吁

- HKTVmall 及集团旗下所有子公司从未聘请刷单员；
- HKTVmall 指定 WhatsApp 账户有蓝剔认证；

- HKTVmall 订单交易都只会于指定网页或应用程序内进行，不会以推广方式邀请客户撰写产品评价，亦不会要求客户收藏产品以提高商户排名；
- 如果雇主要求你在正式上任前垫支费用或保证金，或以「刷单员」、「下单员」、「点赞员」等作招徕，这极可能是骗案；
- 如有怀疑，可致电「防骗易 18222」热线查询。

危險

若你已加入以下群組或下載有關程式

請小心！

因你已經遇上騙子

通訊群組

國海金探通VIP專員
情深即是晚風
港股財經171揭秘老仙股
宏楊學院
聚沙成塔股友交流77
財經佈局交流群

危險

假App

USDT - Metatrader5
Exscion
Bitstorage
DIFX
富達
金沙娛樂城
HR=HL-Semplice
Narkasa
Moderna
澳門巴黎人II

危險

不明連結

gjrapp.com
h5.tokshop56.com
www.xhgj693.com/Public.login.do
app.jcvkgedf.com/
app.gtydgfh.com
cjvipaa68.com
cjvipyy123.com
singapore4d.online
dasator.com/h5
www.bsproex.com
hlhr-stock.com/
app.jcvkgedf.com
xinpujing668.xyz
www.proexu.pro/mobile
h5.actrade.vip
www.proexu.pro/mobile
h1hrapp.com
6rld2.scafyhm.com/tucm4
galaxy-11.top

危險

不明連結

app.ethicn.com/home
mexczx.cn
vrcoin.cloud
www.siqwejja.com
bitstorageep.com/h5
bika/wealthred.com
app.xinsgcbhvg.com
zicoleo.com.h5
app.csasea.cc
narkasaep.com
m.965825.vip
hlhrapp.com
www.modernas.ltd
www.ahaosheng.com/appff
zhonghuat.com
web389.vip
balirenxgvip88.com
w.btforexm.com/h5
web389.vip/

小心！小心！小心！

实时通讯群组

国海金探通 VIP 专员，情深即是晚风，港股财经 171 揭秘老仙股，宏杨学院，聚沙成塔股友交流 77，财经布局交流群

假 App

USDT - Metatrader5，Exscion，Bitstorage，DIFX，富达，金沙娱乐城，HR=HL-Semplice，Narkasa, Moderna，澳门巴黎人 II

不明连结

gjrapp[.]com	bitstorageep[.]com/h5
h5.tokshop56[.]com	bika/wealthred[.]com
www.xhgj693[.]com/Public.login.do	app.xinsgcbhvg[.]com
app.jcvkgedf[.]com/	zicoleo.com[.]h5
app.gtydgfh[.]com	app.csasea[.]cc
cjvipaa68[.]com	narkasaep[.]com
cjvipyy123[.]com	m.965825[.]vip
singapore4d[.]online	hlhrapp[.]com
dasator[.]com/h5	www.modernas[.]ltd
www.bsproex[.]com	www.ahaosheng[.]com/appff
hlhr-stock[.]com/	zhonghuat[.]com
app.jcvkgedf[.]com	web389[.]vip
xinpujing668[.]xyz	balirenxgvip88[.]com
www.proexu[.]pro/mobile	w.btforexm[.]com/h5
h5.actrade[.]vip	web389[.]vip/
www.proexu[.]pro/mobile	app.ethicn[.]com/home
h1hrapp[.]com	mexczx[.]cn
6rld2.scafyhm[.]com/tucm4	vrcoin[.]cloud
galaxy-11[.]top	www.siqwejja[.]com

警方呼吁

- 切勿随意点击可疑短讯、电邮或网页内的超链接，以登入任何网站或下载附件；
- 市民应通过已注册投资机构进行投资；
- 市民可于证券及期货事务监察委员会（证监会）网页查阅持牌人及注册机构的公众纪录册；
- 市民亦可使用守网者网站「防骗视伏器」或「防骗视伏 App」手机应用程序，查核可疑电话号码、网址或收款账号；
- 提醒身边亲友慎防受骗；
- 如有怀疑，可致电「防骗易 18222」热线查询。

反诈骗协调中心及证监会提醒投资者注意社交媒体上的骗局

昨日，反诈骗协调中心与证监会发布了一段由双方联合制作的短片，提醒公众小心网上投资骗局。

该段短片提醒投资者提防有骗徒在社交媒体平台上建立投资群组，并声称能提供股票贴士或内幕消息。在某些个案中，这些骗局更涉及冒认知名的投资顾问和市场评论员。

短片以戏剧形式讲解典型的“唱高散货”计划。“唱高散货”是操纵股票市场的手法之一。骗徒将股票的价格人为地“推高”，并利用社交媒体诱使投资者以高价买入，然后骗徒在高价卖出或“抛售”图利。在大多情况下，投资者并不知悉诱使他们跌入陷阱人士的真实身分。

欢迎市民按动以下连结观赏上述短片:

https://www.facebook.com/HongKongPoliceForce/videos/404394320626114/

手法

近日，警方发现载有高官及名人（包括行政長官及财政司司長）相片的虚假投资广告及网站，诱使市民点击，继而连接到可疑交易平台。相关部门已严正澄清，该广告及有关言论全属虚构。警方正跟进及调查事件。

防骗锦囊

- 如发现有关名人投资成功的报导／广告，应主动核实其真伪。切勿点击该报导／广告或所附连结；
- 切勿在来历不明的网站或应用程序输入自己的信用卡数据、网上银行账户资料或电子货币包数码锁匙（Digital Key）；
- 虚假投资网站一般有错别字、无效链接或语法不通等问题，市民应多加留意；
- 如所谓「投资公司」透过个人银行账户或电子货币包收取投资资金，这极可能是骗局；
- 如有怀疑，应致电「防骗易 18222」热线查询。

什么是 WhatsApp 户口骑劫?

骗徒会用欺骗方式骑劫受害人的实时通讯程序如 WhatsApp 的帐户及通讯簿，继而冒认受害人要求其亲友代买游戏点数卡。

一、 骗取验证码

假冒受害人亲友向他们发出讯息要求受害人转发 WhatsApp 户口之验证码

二、骑劫户口

骗徒以受害人的电话号码登入其 WhatsApp 户口，从而骑劫受害人的账户

三、骗取点数卡

骗徒冒认受害人并向其亲友发送讯息，要求他们代买游戏点数卡，并将点数卡序号发送给骗徒

防骗建议

- 启动实时通讯程序内的双步骤验证功能
- 切勿随便提供实时通讯程序验证码予任何人，以免账户被盗
- 如有亲友透过社交媒体或实时通讯程序要求帮忙购买点数卡或汇款，应确认其身份
- 如有怀疑，可在「防骗视伏器」输入电话号码、社交媒体账号等评估风险，或致电18222查询

https://youtu.be/hRNn2DRfHYA

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

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

2023 版 - 数码 KEY 睇紧啲，撳 LINK 前要三思！

https://www.youtube.com/@HKMASmartTips

喺金管局同香港银行公会嘅推动下，全港 23 间发卡银行同多间主要大型商户已参与《保障消费者防诈骗约章》，承诺唔会透过实时电子讯息 send link 问你攞信用卡同个人资料，记得千祈唔好乱撳 link！ 想知多啲，Click 入以下网址：https://bit.ly/47GdsQx

假冒「防骗视伏器」钓鱼诈骗

手法

近日有骗徒向市民发送钓鱼短讯，声称已追回五千多万「骗金」，诱骗收讯人点击连结进入钓鱼网站下载假「防骗视伏 App」，并输入手机号码和密码。

警方呼吁

请留意，「防骗视伏 App」绝对不会获取用户的个人资料，亦不设登入功能。市民在假App 开设帐号后，可能有假冒内地执法人员讹称可取回诈骗损失，并要求市民把部分损失金额存入骗徒户口，作为手续费。

「防骗视伏器」没有独立网址，市民进入守网者网站（https://cyberdefender.hk）首页，便可免费使用「防骗视伏器」。市民亦可在官方应用程序市场输入「防骗视伏 App」或「Scameter+」，或点击以下安全连结下载「防骗视伏 App」：

苹果 「App Store」

安卓 「Google Play 」商店

华为 「App Gallery」

了解更多：https://cyberdefender.hk/scameter

提防假冒保安局电话骗案

手法

近日，多名市民收到自称保安局职员来电（显示为 8 位数字的本地电话号码），指市民于内地登记的电话号码曾经在社交媒体发放有关俄乌战争相片、影片及呼吁市民捐款筹募等讯息，涉嫌干犯内地法律。操流利普通话的骗徒要求市民提供个人资料或亲身前往保安局办公室以核实身份。对话期间，部份骗徒能够说出市民的姓名。

警方呼吁

- 不要单凭来电者提供的机构名称、电话号码、传真号码或职员编号等去识别其身份；
- 市民若接获有关的可疑来电，必须保持警惕，核实来电者的身份；
- 切勿随意向来电者透露个人资料：包括身份证号码、银行帐户号码及密码等；
- 提醒身边亲友慎防受骗；
- 如有怀疑，可致电「防骗易 18222」热线查询。

伪冒警务处发送钓鱼短讯

手法

近日，有骗徒假冒香港警务处发出欺诈钓鱼短讯，声称警方破获诈骗案并追回八千万骗款，诱使市民点击短讯内附恶意连结，进入预设伪冒网站。

市民进入伪冒网站后，骗徒可能要求市民输入个人或银行账户数据，或透过恶意软件入侵市民的手机系统以偷取重要信息，作诈骗用途。

市民需留意，香港警务处不会透过短讯要求受害人点击任何网址连结！

警方呼吁

- 请勿随意点击可疑短讯、电邮或网页内的超链接，以登入任何网站或下载应用程序；
- 请勿在不明来历的应用程序或网站，输入个人、信用卡、银行账户数据、信用卡三位数安全码(CVC/CVV)或一次性密码；
- 如欲查询案件进度，请联络案件主管或分区警署；
- 提醒身边亲友慎防受骗；
- 如有怀疑，可致电「防骗易 18222」热线查询。

提防伪冒中国互联网违法和不良信息举报中心诈骗电话

手法

近日，多名市民向警方报称收到自称**中国互联网违法和不良信息举报中心**（举报中心）职员的预录语音或真人来电。骗徒以流利普通话或广东话致电，冒充举报中心职员，并讹称市民身份被盗用以注册微信号并发放售卖假药及诱骗公众到东南亚国家从事诈骗等工作的讯息。其间，骗徒要求市民向内地执法机构举报及澄清，并将电话转驳至另一名假冒内地执法人员的骗徒。骗徒表示市民因干犯洗黑钱罪行，需提供个人资料、银行帐户号码及密码，甚至要求市民汇款作保证金或手续费。

警方呼吁

- 如收到声称内地举报中心职员来电，应提高警觉；
- 切勿轻信陌生来电或向陌生人透露个人资料、银行帐户号码及密码；
- 即使陌生人能说出你的个人资料，或传送载有你相片的法律档，亦不代表他是真正的执法人员，因为骗徒可以透过非法手段取得市民的个人资料；
- 如遇到有人自称执法人员或政府机构职员，应提高警觉，主动查证及再三向相关机构核实来电者的身份；
- 提醒身边亲友慎防受骗；
- 如有怀疑，可致电「防骗易 18222」热线查询。

提高警觉：2023 年第二期消费券 - 联络登记人的特定电话号码列表

近日，有市民表示收到骗徒假冒消费券计划秘书处或承办商的来电或短讯(来电显示为 8 位数字的本地电话号码)，讹称市民已被取消「2023 年第二期消费券计划」之资格并要求市民提供个人资料。

2023 年第二期消费券计划已将于星期二（六月二十七日）截止登记，政府会对所有登记人作资格审核。在资格审核的过程中，消费券计划秘书处或其承办商会进行抽查并联络登记人。市民请留意以下事项：

- 致电登记人时不会播放电话录音；
- 所有短讯不会提供任何网站连结；
- 不会向登记人直接索取个人资料；以及
- 政府或承办商只会通过以下特定电话号码致电或发出短讯，如下：

（I）致电登记人

	特定电话号码
消费券计划秘书处	3852 7500 或 2241 9400
获政府委聘就登记人资格进行抽查的承办商 德勤．关黄陈方会计师行	2852 1009

（II）向登记人发短讯

	特定电话号码
消费券计划秘书处	852-6059 1120 或 852-2241 9400

获政府委聘就登记人资格进行抽查的承办商 德勤．关黄陈方会计师行	852-5567 3873
获政府委聘处理／检查表格的承办商 SPS UK&I Limited 凸版信息（香港）有限公司	852-6115 1226 34849 852-6522 4964

所有登记人会收到其审核结果的短讯通知，有关的短讯会以特定电话号码（852 6059 1120）发出。市民亦可透过消费券计划热线 18 5000 的语音系统查询其审核结果。

警方呼吁

- 如收到声称消费券计划秘书处职员来电，应提高警觉，切勿轻信。如对方以不同理由向你索取个人或财产资料，你应该主动向秘书处查证；
- 如市民对电话或短讯的真确性有怀疑，可致电消费券计划热线 18 5000 查询；
- 切勿向来电者透露个人资料：包括身份证号码、储值支付工具账号、银行账户号码及密码等；

- 提醒身边亲友提防受骗，尤其家中长者；
- 如有怀疑，可致电「防骗易 18222」热线查询。

有关政府消费券计划联络登记人的特定电话号码列表，可参阅以下网址：

https://www.consumptionvoucher.gov.hk/tc/information_list.html

假冒官員電話騙案

咪亂聽！
咪亂聽！
咪亂聽！

1 預錄語音 — 騙徒以預錄語音致電市民

2 聲稱市民涉及刑事案件 — 聲稱市民在內地犯法被轉駁至**假冒的內地執法人員**

3 操控網上理財戶口及轉走存款 — 要求**下載應用程式**或到**偽冒網站**最終被**轉走戶口內所有存款**

ADCC Anti-Deception Coordination Centre 反詐騙協調中心

懷疑受騙 即打 18222

想知點拆解伏位？即上 www.adcc.gov.hk

網戀投資騙案

1 搭訕 — 騙徒扮成「**高富帥**」透過社交媒體或交友程式向受害人搭訕

2 網戀投資 — 用甜言蜜語，令受害人以為自己是網上情人，說服受害人下載**一些虛假的投資應用程式**，並聲稱有內幕貼士

3 WIN LOSE 累積輸贏 — 受害人依照**貼士**投資，最終**不能取回投資金額和利潤**

ADCC Anti-Deception Coordination Centre 反詐騙協調中心

懷疑受騙 即打 18222

想知點拆解伏位？即上 www.adcc.gov.hk

投资「A 股」要小心

手法

近日，有不法之徒假扮投资专家，以内幕消息、低风险、高回报作招徕，透过短讯或实时通讯软件招揽市民加入投资教室群组，诱使市民点击不明连结下载虚假「A 股通」手机应用程序，或进入虚假「A 股通」网站开立户口。其后，骗徒要求他们将本金转账至不明个人银行户口。

交易初期，骗徒或会发放小量回报，或透过投资程序 / 网站发放虚假获利记录，以骗取受害人信心，诱使其加大投资金额。骗徒取得大额款项后，便逃之夭夭。

市民可收听「香港电台」于 2023 年 4 月 25 日播出的新闻节目《一桶金之财经新思维》。香港证券及期货专业总会会长陈志华在节目中分享有关投资 A 股的注意事项。

警方呼吁

- 切勿随意点击可疑短讯、电邮或网页内的超链接，以登入任何网站或下载附件；
- 市民应透过已注册投资机构投资沪港通和深港通；
- 市民可于证券及期货事务监察委员会（证监会）网页，查阅持牌人及注册机构的公众纪录册；
- 市民亦可使用守网者网站「防骗视伏器」或「防骗视伏 App」手机应用程序，查核可疑电话号码、网址或收款账号；
- 提醒身边亲友慎防受骗；
- 如有怀疑，可致电「防骗易 18222」热线查询。

相关连结:

《一桶金之财经新思维》
https://podcast.rthk.hk/podcast/item.php?pid=308&eid=218949&lang=zh-CN

持牌人及注册机构的公众纪录册
https://www.sfc.hk/TC/Regulatory-functions/Intermediaries/Licensing/Register-of-licensed-persons-and-registered-institutions

「防骗视伏器」
https://cyberdefender.hk/scameter/

钓鱼攻击

什么是钓鱼攻击？

钓鱼攻击（Phishing attack），又称「网络钓鱼」，是流行的网络犯罪手段。黑客以渔翁撒网方式发放伪装由政府、银行、网上付款服务商、网上零售商或公司商业伙伴等机构的电邮或短讯，内含的连结或二维码所指向的钓鱼网站与真实网站极度相似，从而诱使收件者输入登入密码、个人资料、信用卡数据等。

黑客亦可能会在讯息内嵌链接、二维码或档案附件，如收件者不慎点击链接或开启附件，其装置便可能受恶意软件感染。

黑客最近假冒甚么？

在去年的「网络钓鱼」当中，黑客以假冒金融机构和邮递服务占大多数。

假冒金融机构 / 电子支付平台

- 黑客假冒金融机构，例如银行发出的钓鱼短讯，声称户口有异常或有转账指示，要求用户立即处理或确认。诱骗用户进入假网站并提供手机号码和一次性密码，然后用另一手机骑劫账户并将钱转走。由于骗徒隐藏发讯人的电话号码，并假冒银行昵称，手机系统会把同一昵称发出短讯视为同一人发出，令真假短讯放在一起，令人难以分辨。
- 也有黑客从不同渠道（如系统漏洞、暗网等）取得市民个人资料，假扮银行职员来电，声称要求用户提供「交易密码」及以手机接收「一次性密码」以更新支付平台账户，

否则会冻结其户口。由于骗徒能准确地讲出市民的个人资料，因而容易取得市民信任。取得上述资料后，骗徒随即骑劫户口并将钱转走。

假冒邮递服务 / 公营机构

- 「由于欠缺资料，包裹未能付运」、「未能顺利付款，已暂停有关服务，请更新付款方式」、「Your package with track number xxxx still waiting your instruction (你的包裹编号 XXX 仍等待指示)」，都是假冒邮递服务或电力公司、煤气公司、港铁等公营机构钓鱼讯息的开场白，诱骗用户打开链接进入假网站。由于钓鱼讯息的接口设几可乱真，而且使用了迫切的字眼如「暂停服务」、「会被退件」等，令收件人在情急之下提供个人或信用卡数据。

如何辨识钓鱼攻击？

- 注意发件人的电邮标头，检查电邮地址的域名（domain）是否有异样
- 标题包含「账号即将关闭」等字眼，利用收件者担忧的心理以减低其警觉性
- 电邮内容前后矛盾、文法不通或拼字错误
- 电邮内有可疑连结、二维码或附件
- 伪冒网站的域名与官方网站的域名极为相似（如数字「1」取代字母「I」）
- 伪冒网站或会有部分连结失效

安全贴士

- 不要开启来历不明的邮件或讯息
- 查看清楚发件人的数据
- 切勿点击可疑电邮或讯息内的超链接
- 切勿登入未经查证的网站
- 如网站要求提供个人或信用卡数据，应加倍小心
- 如怀疑受骗，应保存相关电邮或讯息，并尽快报警

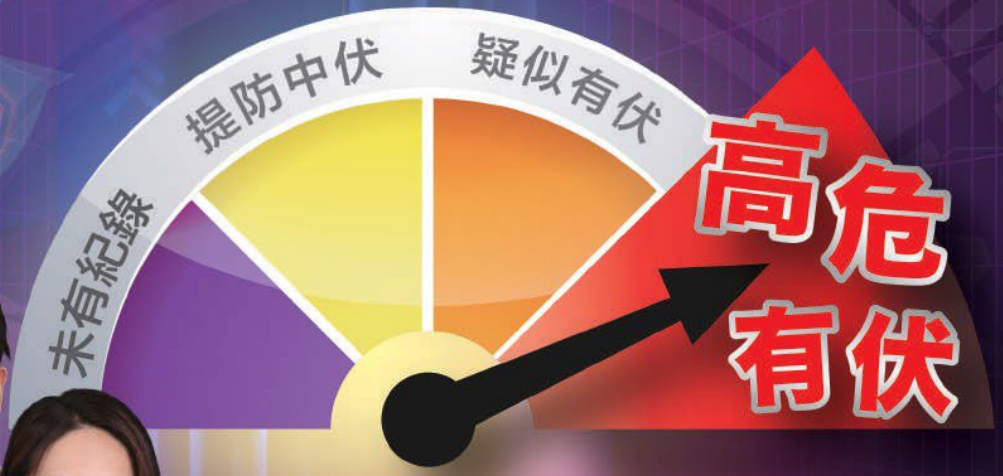

懷疑受騙　即打18222
寂寞
網戀
恐懼
來電靠嚇
貪心
瘋投快搵機
無知
刷單圈套
騙局誘惑
捉心理騙局
誘惑到你萬劫不復！
ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

陌生來電　可疑網店　筍工招聘　白撞訊息　必賺投資

係咪呃緊你？Check 吓

防騙視伏器

即上 CyberDefender.hk



輸入資料，揭穿**詐騙**陷阱！

一站式詐騙陷阱搜尋器

電話號碼
平台用戶名稱
社交帳號
網址
收款賬號
電郵地址
IP 地址

網頁　Facebook　Instagram　YouTube

CYBER 守網者 DEFENDER