FMLIT Publicity Materials for Q4 2023 – 注意！虛假投資理財詐騙渠道

小心！小心！小心！

即時通訊群組

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

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

不明連結

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

警方呼籲

- 切勿隨意點擊可疑短訊、電郵或網頁內的超連結，以登入任何網站或下載附件；
- 市民應通過已註冊投資機構進行投資；
- 市民可於證券及期貨事務監察委員會（證監會）網頁查閱持牌人及註冊機構的公眾紀錄冊；
- 市民亦可使用守網者網站「防騙視伏器」或「防騙視伏 App」手機應用程式，查核可疑電話號碼、網址或收款帳號；
- 提醒身邊親友慎防受騙；
- 如有懷疑，可致電「防騙易 18222」熱線查詢。

FMLIT Publicity Materials for Q4 2023 – 提防「名人效應」投資騙案

手法

近日，警方發現載有高官及名人（包括行政長官及財政司司長）相片的虛假投資廣告及網站，誘使市民點擊，繼而連接到可疑交易平台。相關部門已嚴正澄清，該廣告及有關言論全屬虛構。警方正跟進及調查事件。

防騙錦囊

- 如發現有關名人投資成功的報導 / 廣告，應主動核實其真偽。切勿點擊該報導 / 廣告或所附連結；
- 切勿在來歷不明的網站或應用程式輸入自己的信用卡資料、網上銀行賬戶資料或電子錢包數碼鎖匙（Digital Key）；
- 虛假投資網站一般有錯別字、無效連結或語法不通等問題，市民應多加留意；
- 如所謂「投資公司」透過個人銀行賬戶或電子錢包收取投資資金，這極可能是騙局；
- 如有懷疑，應致電「防騙易 18222」熱線查詢。

反詐騙協調中心及證監會提醒投資者注意社交媒體上的騙局

昨日，反詐騙協調中心與證監會發佈了一段由雙方聯合製作的短片，提醒公眾小心網上投資騙局。

該段短片提醒投資者提防有騙徒在社交媒體平台上建立投資群組，並聲稱能提供股票貼士或內幕消息。在某些個案中，這些騙局更涉及冒認知名的投資顧問和市場評論員。

短片以戲劇形式講解典型的“唱高散貨”計劃。“唱高散貨”是操縱股票市場的手法之一。騙徒將股票的價格人為地“推高”，並利用社交媒體誘使投資者以高價買入，然後騙徒在高價賣出或“拋售”圖利。在大多情況下，投資者並不知悉誘使他們跌入陷阱人士的真實身分。

歡迎市民按動以下連結觀賞上述短片:

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

什麼是 WhatsApp 戶口騎劫?

騙徒會用欺騙方式騎劫受害人的即時通訊程式如 WhatsApp 的帳戶及通訊錄，繼而冒認受害人要求其親友代買遊戲點數卡。

一、 騙取驗證碼

假冒受害人親友向他們發出訊息要求受害人轉發 WhatsApp 戶口之驗證碼

二、騎劫戶口

騙徒以受害人的電話號碼登入其 WhatsApp 戶口，從而騎劫受害人的帳戶

三、 騙取點數卡

騙徒冒認受害人並向其親友發送訊息，要求他們代買遊戲點數卡，並將點數卡序號發送給騙徒

防騙建議

- 啟動即時通訊程式內的雙步驟驗證功能
- 切勿隨便提供即時通訊程式驗證碼予任何人，以免帳戶被盜
- 如有親友透過社交媒體或即時通訊程式要求幫忙購買點數卡或滙款，應確認其身份
- 如有懷疑，可在「防騙視伏器」輸入電話號碼、社交媒體帳號等評估風險，或致電 18222 查詢

https://youtu.be/hRNn2DRfHYA

FMLIT Publicity Materials for Q4 2023 – Online account hijacking

甚麼是網上帳戶騎劫？

早在2014年，已經出現戶口騎劫案件。當時，即時通訊軟件LINE由於有系統漏洞，導致用戶帳號被黑客入侵並騙取通訊錄的親友購買點數卡，有關漏洞直至大約2016年才得以修復。在2017年，有騙徒開始騎劫用戶的WhatsApp帳戶，亦以同樣手法騙取市民購買點數卡，後來WhatsApp推出「雙步驟驗證」（現稱「雙重驗證」）功能，情況才逐步得以改善。

2023年8月開始出現新型帳戶騎劫手法。新手法利用釣魚白撞訊息，後來演變為「搜尋器優化中毒」的攻擊。當中大部分的案件涉及WhatsApp帳戶，亦有小量涉及Telegram和其他網上平台。

手法一：釣魚短訊

- 騙徒發送釣魚短訊，內附連結至假網站
- 假網站套取用戶電話號碼，並要求平台向用戶發放轉移代碼
- 騙徒再向用戶套取轉移代碼
- 騙徒用另一裝置登入用戶的帳戶
- 騙徒向用戶的親友以轉帳或借貸為名騙財

手法二：搜尋器優化中毒攻擊

- 騙徒製作假WhatsApp網頁登入版面網站
- 騙徒在搜尋器以「WhatsApp」作為關鍵字投放廣告
- 用戶在搜尋器輸入關鍵字「WhatsApp」，假網站便會以置頂廣告形式出現
- 用戶點擊置頂廣告進入虛假網站，然後掃描惡意二維碼，騙徒隨即取得用戶連線資料
- 騙徒經網上版WhatsApp同時登入用戶的帳戶，並向親友騙財

其實，網上帳戶入侵可能有不同的原因，例如曾在公用電腦上登入網頁版的即時通訊軟件而忘記登出、使用了惡意的多帳戶登入工具、電子裝置遭到惡意軟件入侵等。

騙徒通常以網上銀行轉帳超出限額為由，要求通訊錄的聯絡人幫忙轉錢，並且承諾翌日還錢，要求轉錢的數目也是由數千至數萬元不等。當然偶爾也有巨額轉帳要求。

提防網上帳戶騎劫的貼士：

啟用雙重認證功能

定期檢視帳戶所連結的裝置，並且登出所有不明的已連結裝置

切勿隨便透露密碼、驗證碼或掃描二維碼

於留言信箱設定強密碼，避免一次性語音密碼被盜取

避免連接公共Wi-Fi或在公共電腦上登入網上帳號

不要盡信搜尋器的結果，建議將常用網頁加入書籤

留意短訊內容和網頁是否有異樣,例如域名串錯字、繁簡字夾雜等

如收到親友透過訊息要求幫忙過數或匯款，應致電對方確認其身份及有關要求

如有懷疑，可在「防騙視伏器」輸入網址、收款帳號等評估風險，或致電18222查詢