

如何識破網絡釣魚攻擊和 保護個人信息



釣魚騙案

- 騙徒漁翁撒網發放虛假電郵和SMS短訊
- 電郵和SMS內帶有連結引領前往虛假網站
- 網站要求輸入帳戶資料、個人資料、信用卡資料等
- 套取帳戶資料後盜用積分換取禮品，信用卡資料用於海外網站購買無實物的貨品轉售圖利或個人資料作不法用途



釣魚騙案

假冒**官員**WhatsApp訊息
盡現關愛  小心**詐騙**！



網上賣嘢都要**銀行密碼**？
擺明又係**假link套料**！



我有興趣買，想安排埋送貨，
你去呢條link入銀行資料，
之後貨到付款。

<http://lalamove.complete-order.shop/26...>



釣魚騙案

真的想釣
yuu?!

假

yuu：您的帳戶 yuu 積分將於今日內到期，請儘快換領獎賞，逾期將作廢 <http://yuurewards9.bond>

異常的
易賞錢短訊

Moneyback：你嘅限時積分已發送至你的會員帳戶，限6個鐘內用！仲唔即刻入嚟掃貨？優惠訂閱回覆1/拒絕訂閱回覆2(如鏈結失效請複製到瀏覽器打開)，連結：parkandshop.info

假

parkandshop.info

騙徒又想開飯喇！

開飯喇-您的OpenRice(1240分)開飯獎賞計劃即將過期，請儘快前往換領禮品
<http://point.openrice1.top>

假

釣魚騙案 防騙貼士

- 不要開啟來歷不明的郵件或訊息
- 查看清楚寄件者的資料及內文有沒有異常 (例如錯字、簡體字等)
- 切勿點擊可疑電郵或訊息內的超連結
- 應向有關機構查證
- 如網站要求提供個人或信用卡資料，應加倍小心
- 使用防騙視伏器或防騙視伏App，輸入可疑電郵地址、電話號碼、網址、收款帳號，可即時評估詐騙風險
- 如懷疑受騙，應保存相關電郵和匯款記錄，並致電18222或報警求助

WhatsApp 戶口騎劫

① 白撞訊息假稱帳號會永久註銷

官方檢測到您的賬號存在安全風險，12小時後將永久註銷，且不可解封；為確保賬號安全，請聯系客服完成以下驗證：whatsapp.org

② 虛假網站要求提供驗證碼



③ 輸入驗證碼後確認連結裝置就會被騎劫



④ 發訊息予親友要求購買點數卡或作其他不法行為



WhatsApp 戶口騎劫 防騙貼士

- 啟用雙步驟驗證及更改PIN密碼
- 切勿隨便提供即時通訊程式驗證碼予任何人
- 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轉賬，應致電確認



你的Whatsapp代碼:199-567
點擊這個鏈接驗證電話號碼:
v.whatsapp.com/199567
請不要和別人共享代碼



電郵騙案 常見手法

- 假冒商業夥伴/供應商要求將貨款存入新戶口
- 假冒公司高層指示員工匯款至不明戶口
- 假冒上司指示員工買iTunes卡
- 假冒商戶發送推廣電郵
- 假冒親戚要求匯款



商業電郵騙案

假冒商業夥伴/供應商 要求將貨款存入新戶口

from: finance@scamc0mpany.com
to: [redacted]
subject: Change of new bank account

Dear Paul,

Please be informed that our company's bank account has just been changed to 888-789-002-00X. Please make your settlement of November to the captioned account.

- 騙徒入侵買賣其中一方郵箱
- 假扮供應商要求買方將貨款存入不明銀行戶口

假冒公司高層 指示員工匯款至不明戶口

from: ceo@scamc0mpany.com
to: [redacted]
subject: Immediate wire transfer

Dear Mary,

Please process a wire transfer payment in the amount of \$250,000 and code to "admin expenses" by COB today. Wiring instructions below.....

- 騙徒入侵公司員工郵箱
- 假扮高層要求財務部同事將貨款存入不明銀行戶口

如何辨別可疑電郵？

- 發件人的電郵地址通常會有異樣，例如字母「L」會寫成「1」；「O」會寫成「0」
- 電郵內容中是否有文法錯誤或拼寫錯誤
- 電郵的商標會否是舊版本、圖像是否解像度低或比例有異常
- 把桌面電腦的滑鼠浮標停在電郵地址或連結之上，便能看到完整電郵地址或連結，幫助了解真偽

真 finance@scancompany.com

假 finance@scamcompany.com

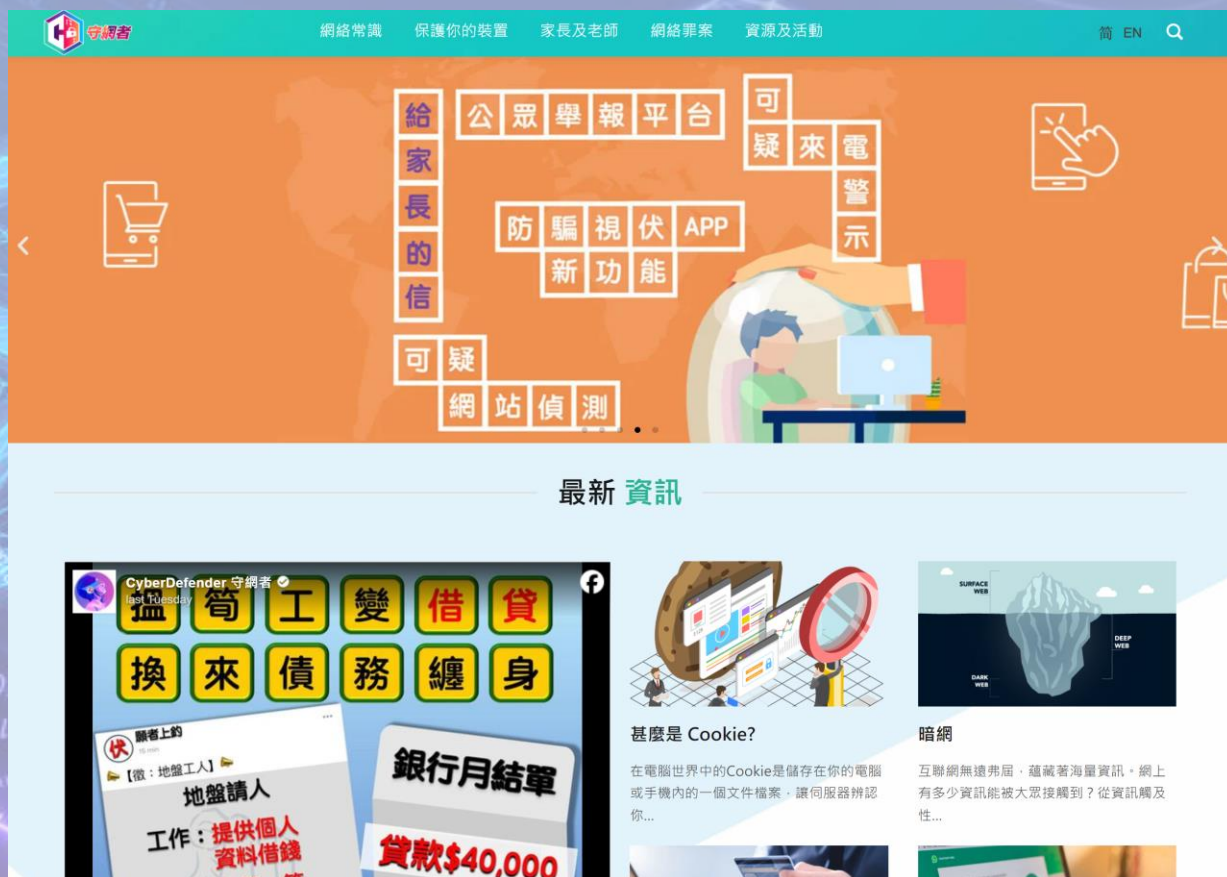
電郵騙案 防騙貼士

- 不要開啟來歷不明的郵件
- 查看清楚寄件者的資料
- 切勿點擊可疑電郵內的超連結
- 切勿登入未經查證的網站
- 不要輕信突然改變的匯款要求；匯款前以電話致電對方核實身分
- 如網站要求提供個人或信用卡資料，應加倍小心
- 使用防騙視伏器或防騙視伏App，輸入可疑電郵地址、電話號碼、網址、收款帳號，可即時評估詐騙風險
- 如懷疑受騙，應保存相關電郵和匯款記錄，並致電18222或報警求助
- 向公司職員 / 商業伙伴傳遞以上資訊

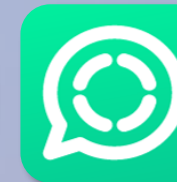


CYBER 守網者
DEFENDER

: 一站式網站及社交平台



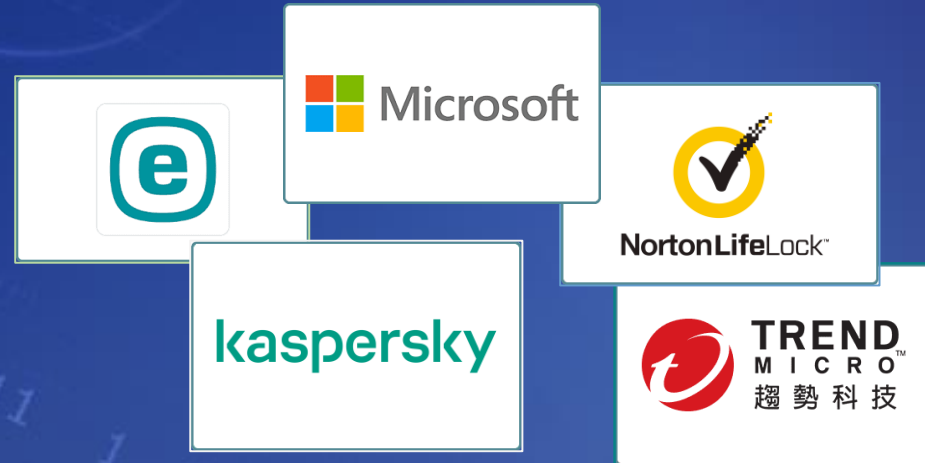
- 提供最新資訊、短片、有聲書、線上遊戲等資源
- 設「家長及老師」專欄



Cyberdefender.hk

電腦設備防護工具

電腦掃描及清洗工具



https://cyberdefender.hk/security_tools/



流動裝置應用程式

防騙視伏器 / 防騙視伏App

 守網者

網絡常識 保護你的裝置 家長及老師 網絡罪案 資源及活動

簡 EN 

疑似詐騙 / 網絡陷阱？
用「防騙視伏器」Check吓啦！

請選擇類型

請選擇類型
平台帳戶名稱
平台帳戶號碼
電話號碼
電郵地址
網址
收款賬戶
IP 地址
雜湊值



如不確定資料類型，便無需選擇。



立即下載最新防騙視伏App
自動「偵伏」舉報「騙局」



Cyberdefender.hk





一站式詐騙陷阱搜尋器



疑似遇到詐騙？用「防騙視伏器」Check吓啦！



可疑來電警告
開啟



可疑網站偵測
開啟



公眾舉報平台
已登記

最後更新: 2024-06-18 18:06

 守網者

 最新消息

 主頁

 來電管理

 設定

防騙視伏器 / 防騙視伏App 搜尋結果



紅色代表「高危有伏」：
輸入的資料與詐騙舉報有關，或網絡安全風險屬高危級別



橙色代表「疑似有伏」：
有相近的詐騙舉報資料，或網絡安全風險屬中高級別



黃色代表「可能有伏」：
你仍需提防中伏



紫色代表「未有記錄」：
但不代表無伏，應時刻保持警惕

留意可疑帳號警示



轉數時 要醒啲

提示！有警示，
都唔等於一定安全㗎！

G.E.M. 鄧紫棋

立即了解



CyberDefender.hk

可疑識別代號警示 簡介

市民透過主要銀行及儲值支付工具（電子錢包）透過轉數快平台進行本地轉帳時，如輸入的轉數快識別代號，包括：



手提電話號碼



電郵地址

1234567

轉數快識別碼

與詐騙舉報有關，並在警方的「防騙視伏器」內標籤為紅色「**高危有伏**」，市民便會在確認交易的頁面收到可疑警示，提醒他們有關轉帳存在高度詐騙風險。

高危警示 樣本

//// //// 警示 ////

根據香港警務處在「防騙視伏器」上提供的防騙資訊，此「轉數快」收款識別代號(手機號碼/電郵地址/快速支付系統識別碼)被列為「**高危有伏**」。

請您在進行交易前再次查證收款人實屬可靠。

取消交易

繼續交易



Facebook



Instagram



YouTube