預防網絡安全威脅

Preventing Cyber Security Threats

數字政策辦公室
項目管理及網絡安全部

Digital Policy Office
Project Governance and Cybersecurity Division

Jan 2026

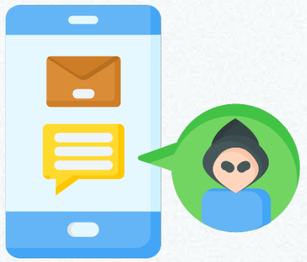
主題

釣魚攻擊 (Phishing)

數字政策辦公室資訊保安推廣活動

什麼是釣魚攻擊(Phishing)？

網絡釣魚攻擊是一種欺騙手法，利用以假亂真的方式騙取受害人的個人資料，甚至金錢。常見的釣魚手法是攻擊者透過電郵、短訊或即時訊息，冒充你認識的人或信任的機構，引導受害人提供敏感資料或開啓惡意網站或附件。



常見釣魚詐騙手法


由於郵費不足，我們無法交付你的包裹：DG-redlivery.com
話要額外郵費先再派件，照做就俾人盜用咗信用卡！


你的積分將於今日到期作廢，請立即換領獎賞。
https://wuurewards.top
諗住加錢換野啫...點解我啲積分會無晒㗎？


您的銀行賬户顯示異常，請立即登入更新用户資料，否則賬户將立即被凍結
http://fortunebamk.com
銀行有一大筆存款轉走咗嘅...


高薪兼職，在家辦公，無需經驗。歡迎申請加入我哋！
wryip.jobs
JOB
無糧出！
仲盜用我嘅銀行資料同身份證申請信貸？

為什麼老師特別容易成為攻擊目標？

- 持有大量學生與家長的聯絡資料
- 通常擁有校內系統存取權限
- 工作繁忙、郵件往來頻繁
- 經常接收來自陌生人（家長、比賽機構、活動單位）的郵件
- AI 技術讓偽造語音、網站越來越逼真

潛在風險



- 學生、甚至家長的個人資料外洩
- 校內系統遭勒索，伺服器被加密導致癱瘓
- 冒用你的老師身份進行詐騙，例如向家長收「書簿費/活動費」

識別釣魚詐騙！

偽冒寄件者
Fake sender

文法錯誤
Grammatical error

具誤導性超連結
Misleading link

【FutureBank】
恭起您！您已獲得 $10000 的信用獎賞。
請 立 即 登 入 您 的 銀 行 帳 戶
www.futurebamk.top 領取獎賞。否則，
您的獎賞將被取消。

Congretulations! You have won a $10000 credit reward. Please login your bank a/c www.futurebamk.top to claim your reward immediately. Otherwise, your reward will be cancelled.

難以置信的獎賞
Unrealistic reward

不尋常的要求
Unusual request

語調緊急
Urgent tone

釣魚電郵例子

1 陌生寄件人或不明的電郵地址

From: eTicket - HSBC
Subject: eSignlive : New document to be signed

HSBC hereby invites you to digitally sign the following agreement documents.

Log in to view agreements and sign documents in an easy and secure way.

Go to documents

汇丰银行特此邀请您对以下协议文件进行数字签名

登录以轻松安全地查看协议和签署文档。

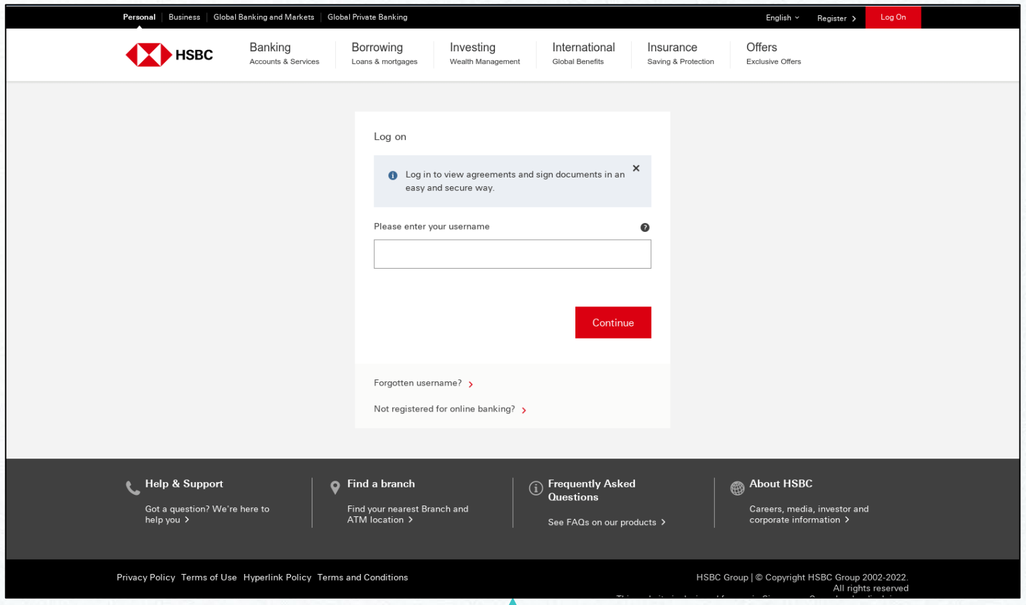
转到文档

2 要求輸入個人 / 敏感資料

3 帶誤導性超連結

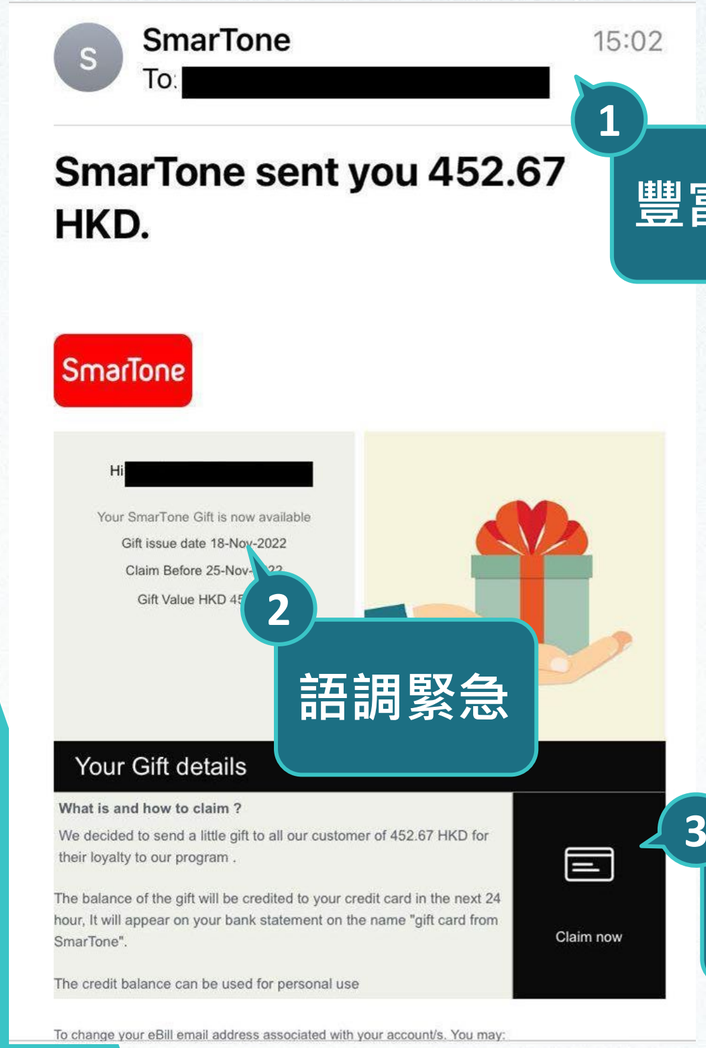
Phishing email

alfalahkita[.]com[/]mobile[/]key[/]login.php



資料來源 Source：https://www.hsbc.com.hk/zh-hk/help/cybersecurity-and-fraud/phishing/

釣魚電郵例子

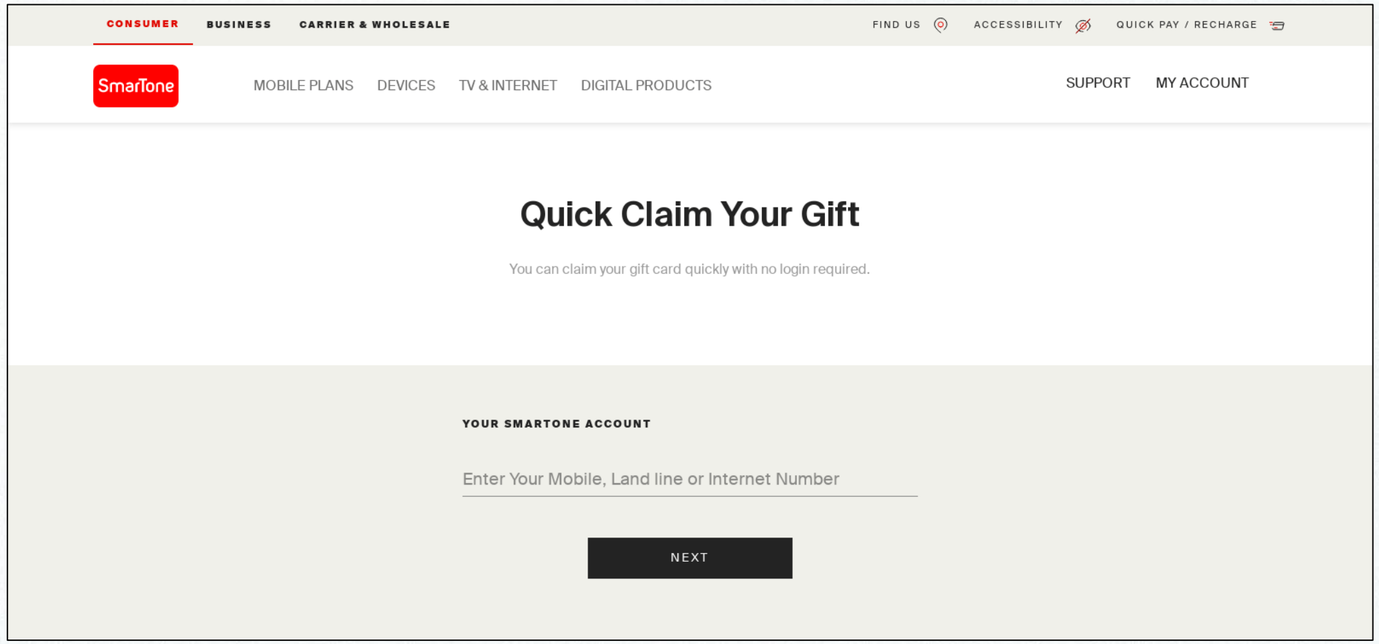


1 豐富獎賞

2 語調緊急

3 帶誤導性超連結

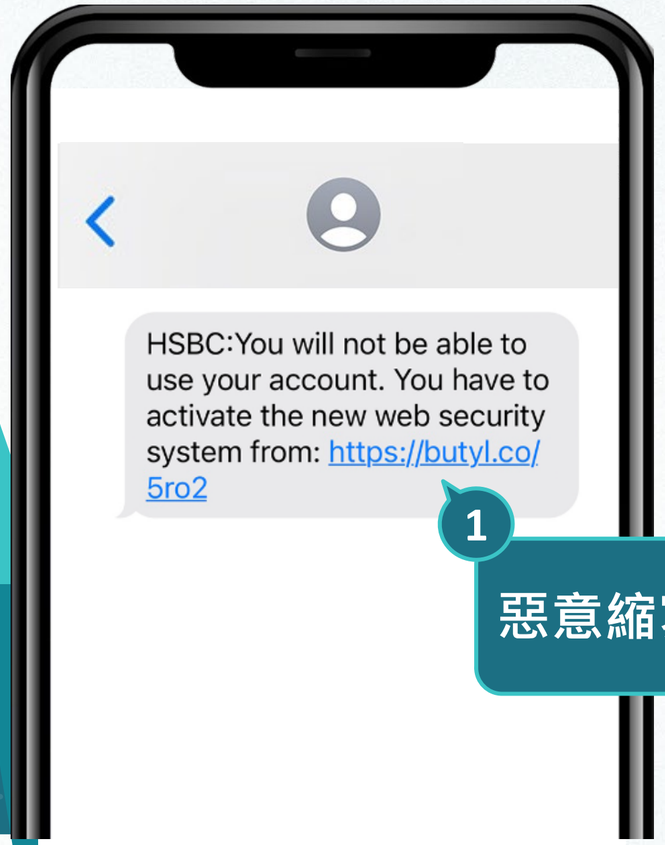
smartone[.]egift-claim.hk[.]gunaysigorta[.]com[/]amount=452.67



資料來源 Source: 香港網絡保安事故協調中心 (HKCERT)

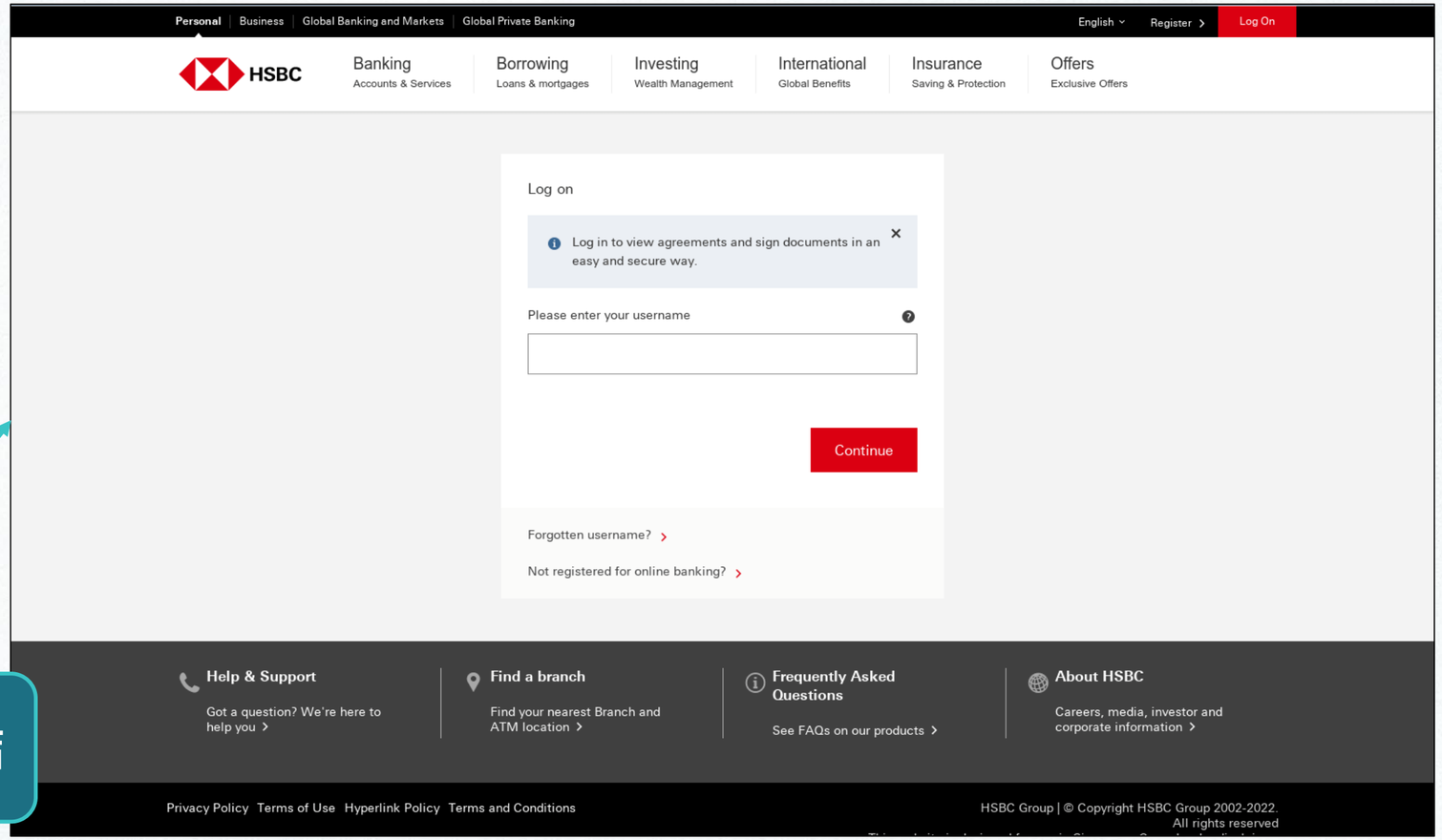
釣魚短訊例子

alfalahkita[.]com[/]mobile[/]key[/]login.php



1

惡意縮寫URL連結



資料來源 Source：https://www.hsbc.com.hk/zh-hk/help/cybersecurity-and-fraud/phishing/

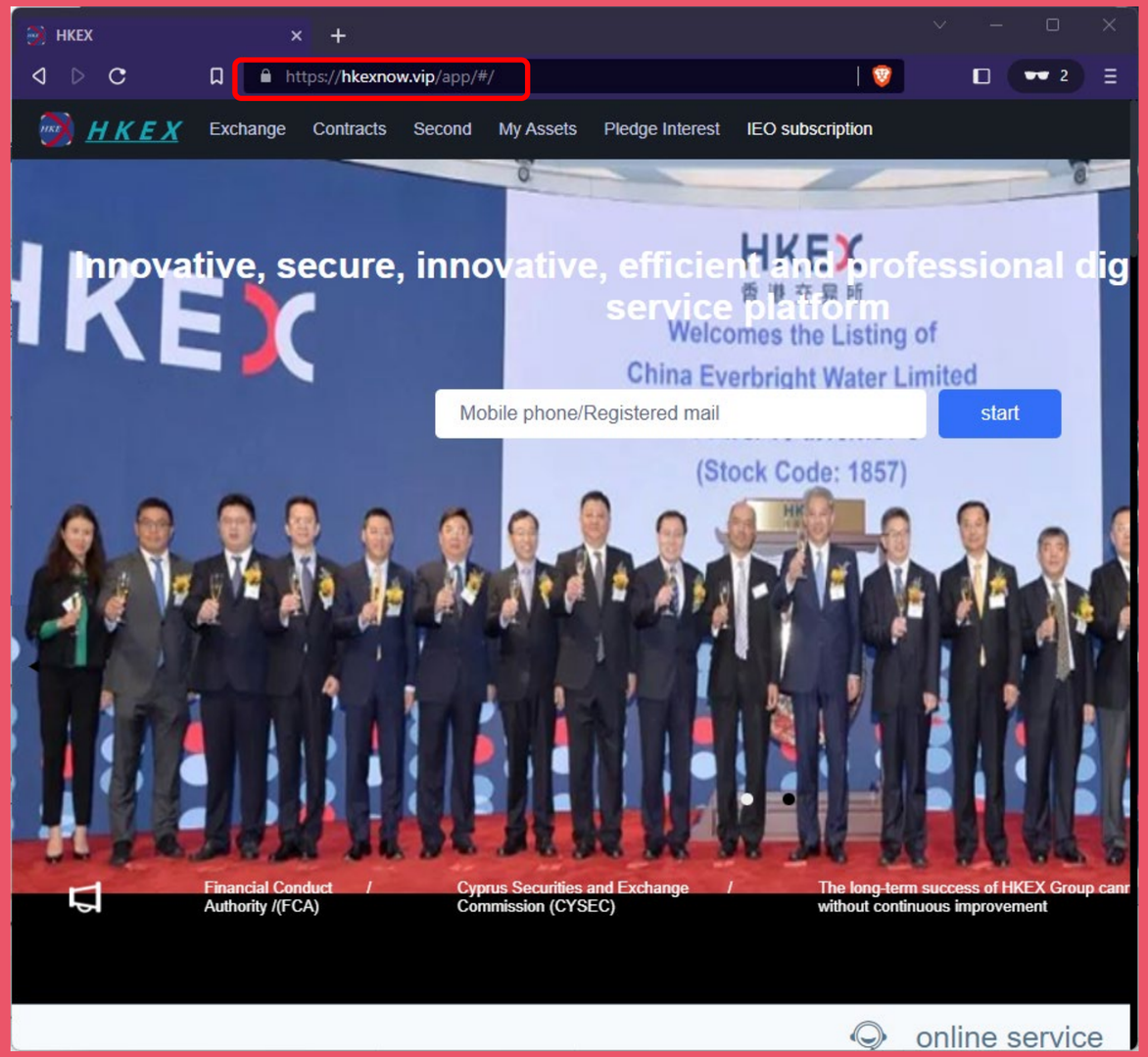
釣魚網站的特徵

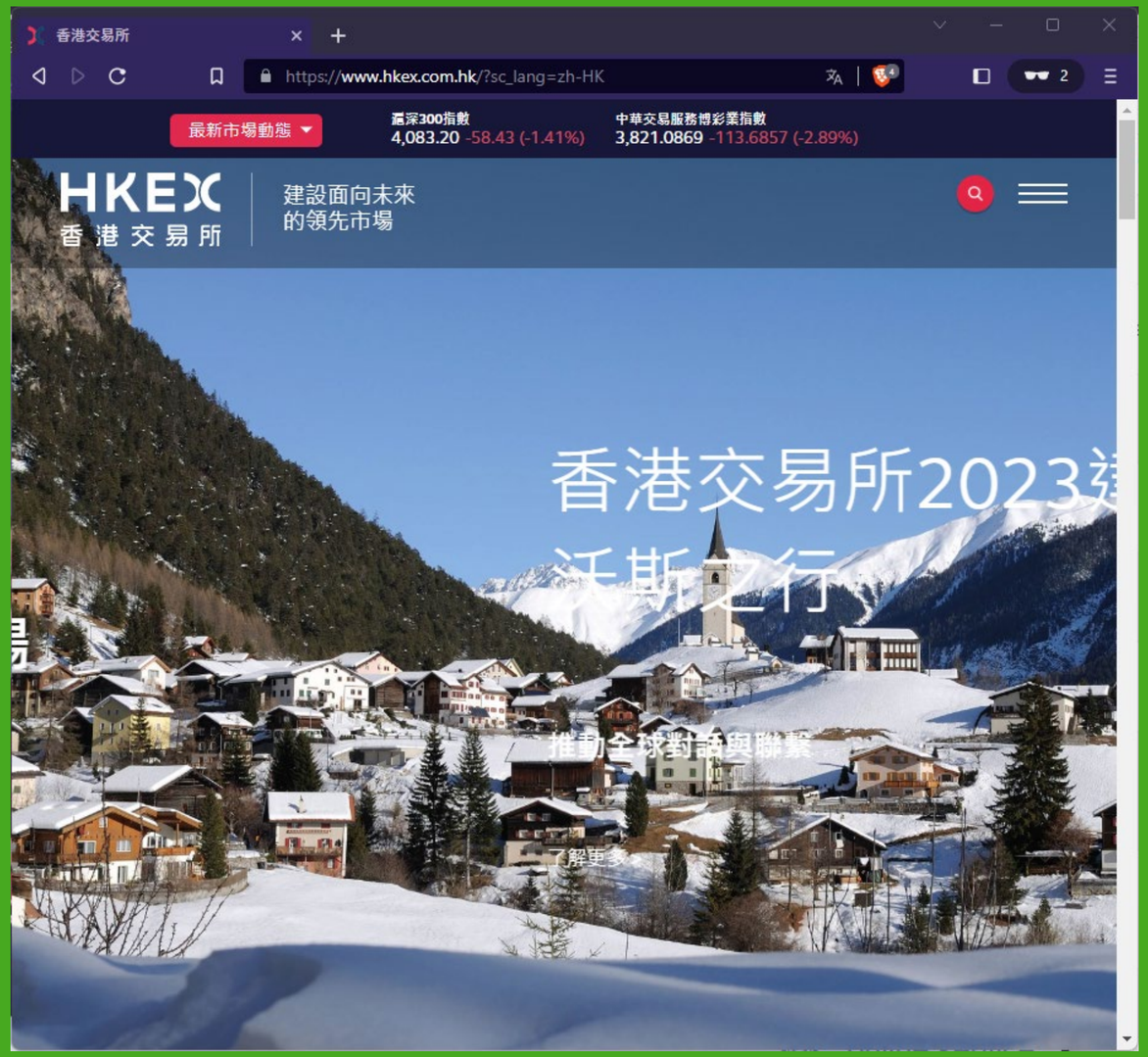
資料來源 Source: https://www.bochk.com/en/aboutus/fraudalert.html

釣魚網站的特徵

資料來源 Source: https://www.bochk.com/en/aboutus/fraudalert.html

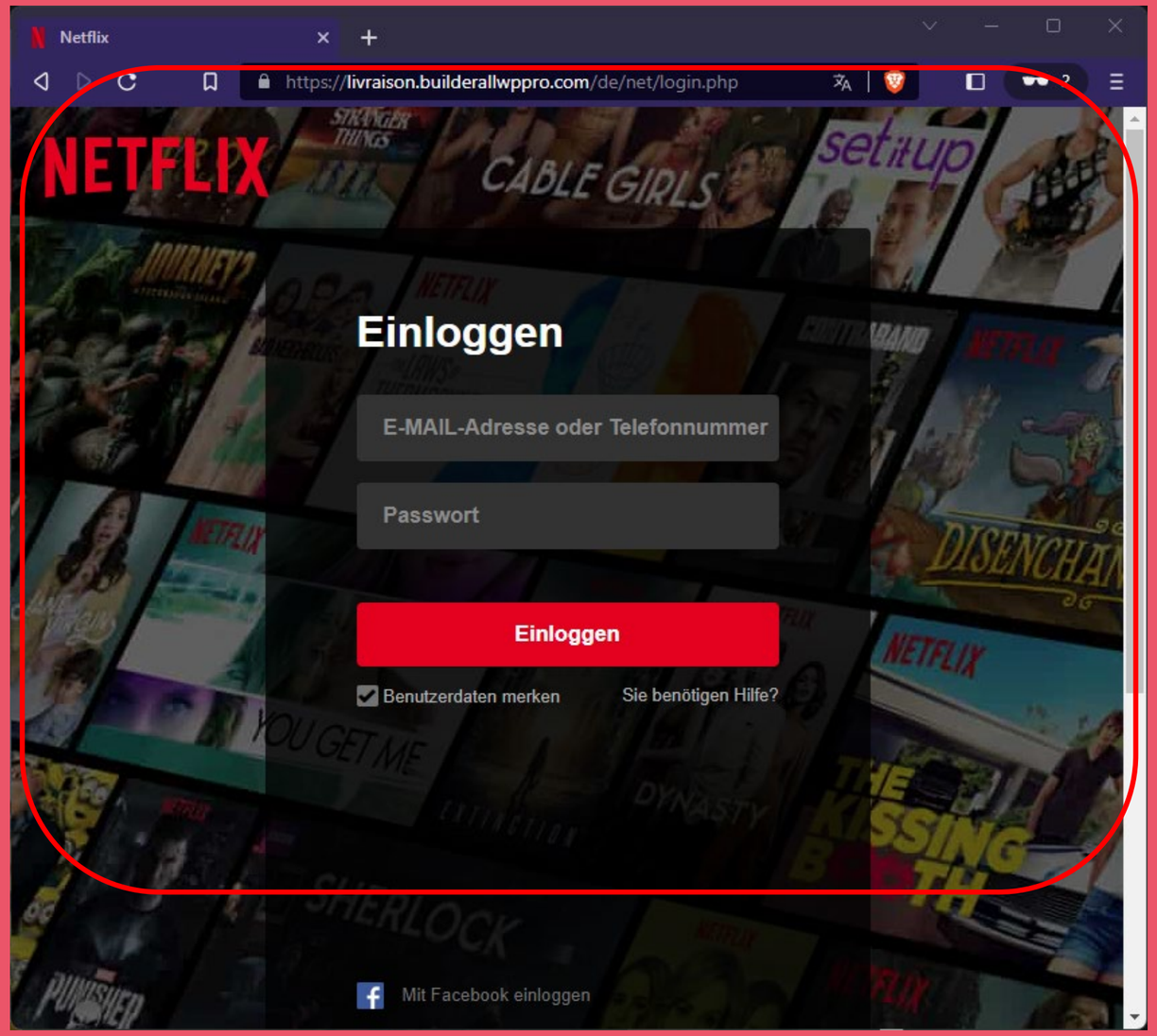
與真實網址相似

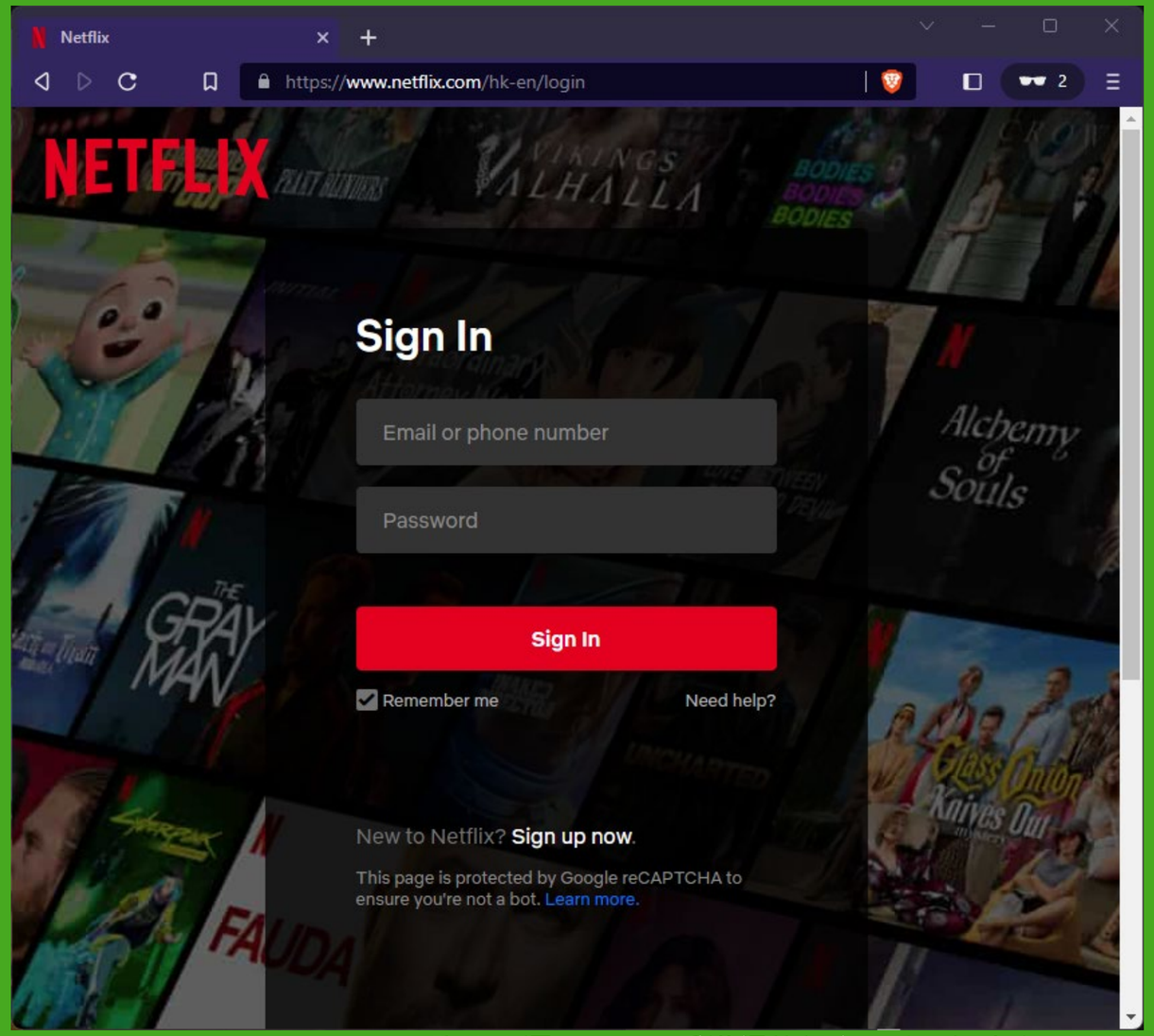




資料來源 Source: https://www.hkex.com.hk/Global/Exchange/Alert?sc_lang=zh-HK

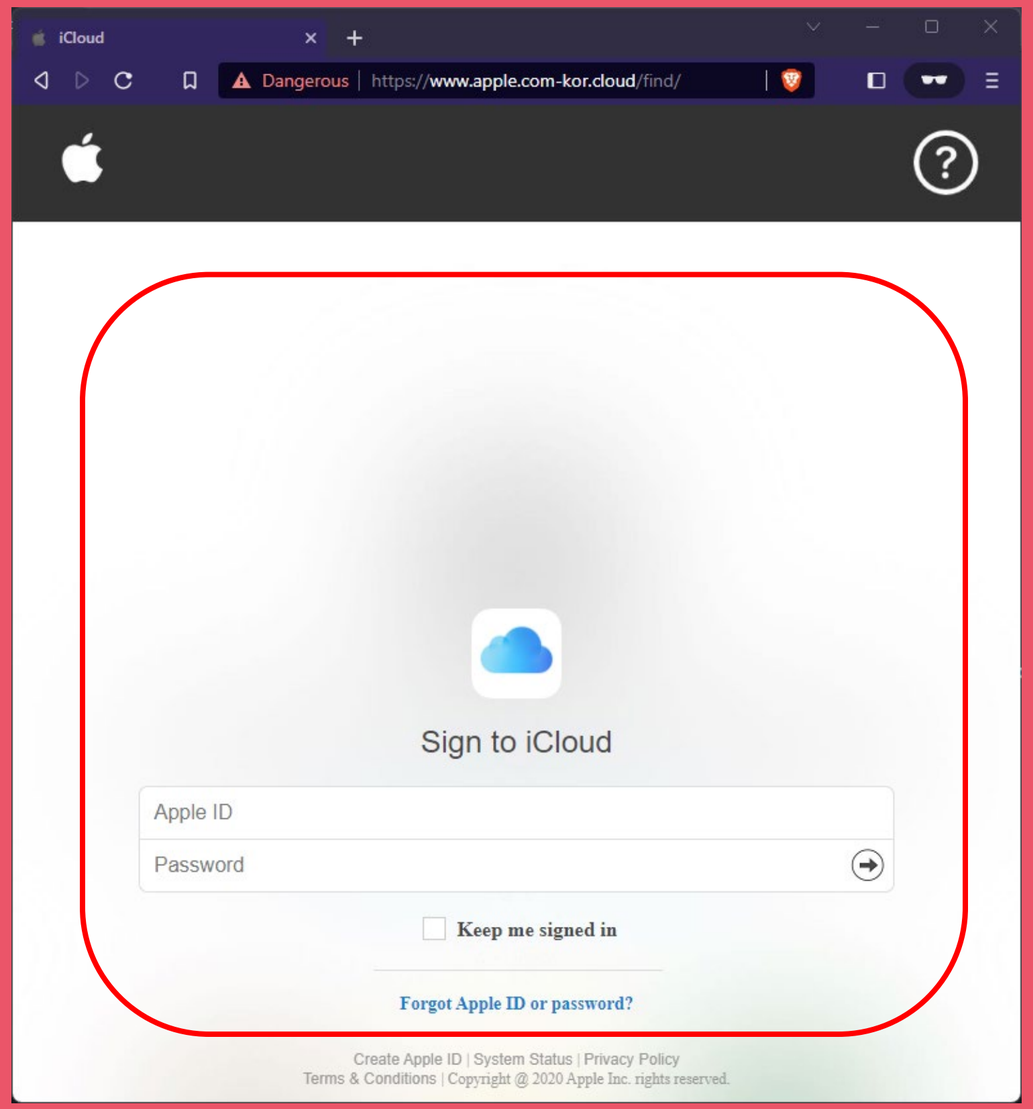
複製真實網頁介面

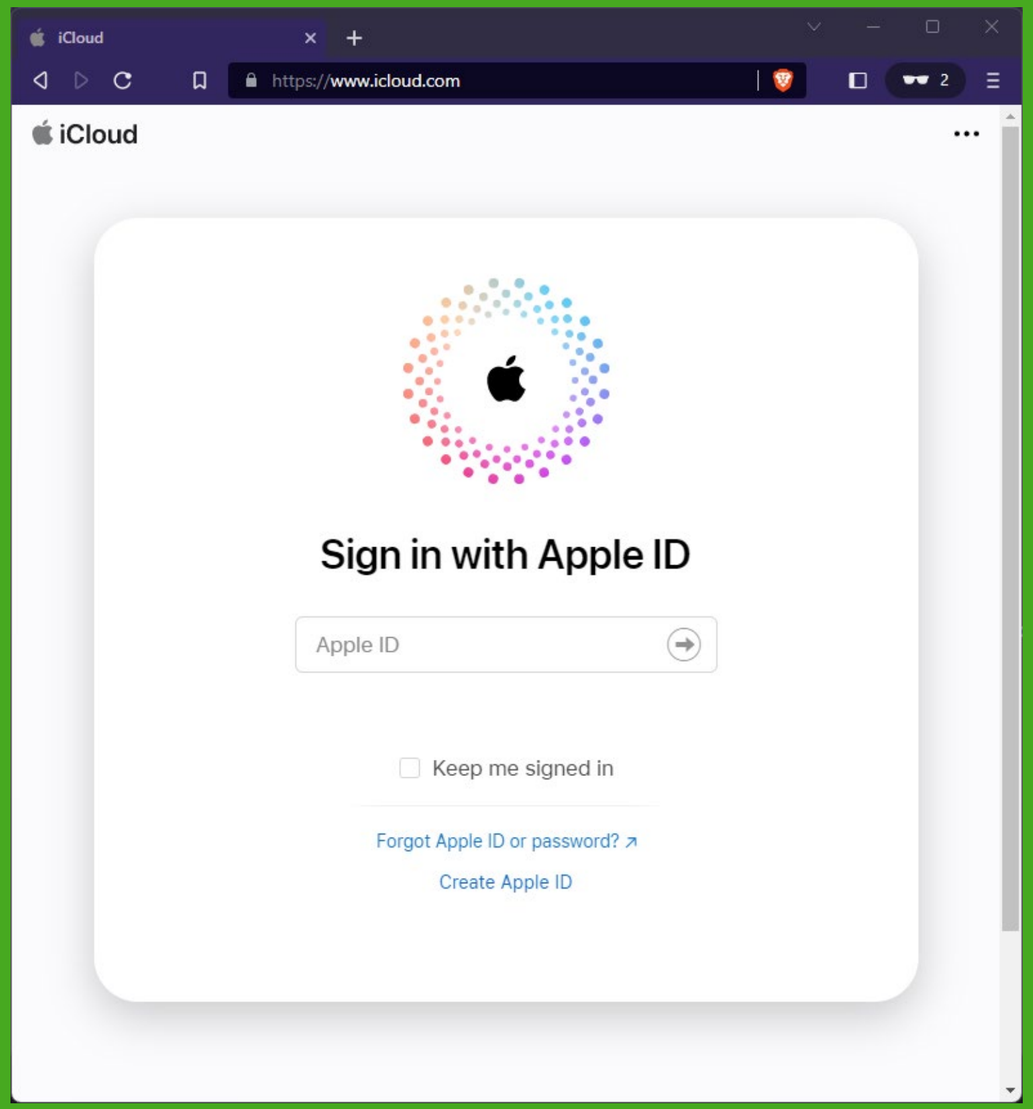




資料來源 Source: 香港網絡保安事故協調中心 (HKCERT)

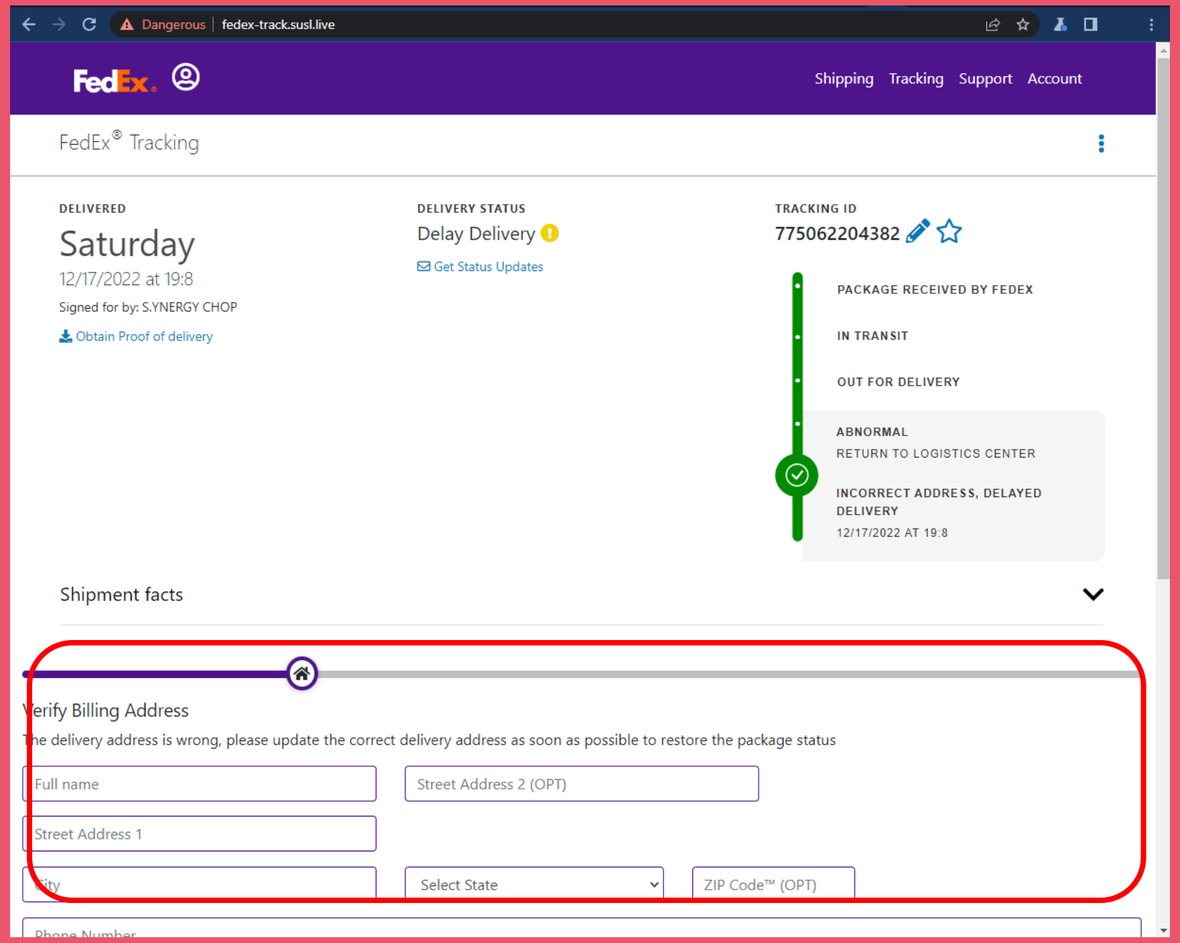
視覺設計不佳

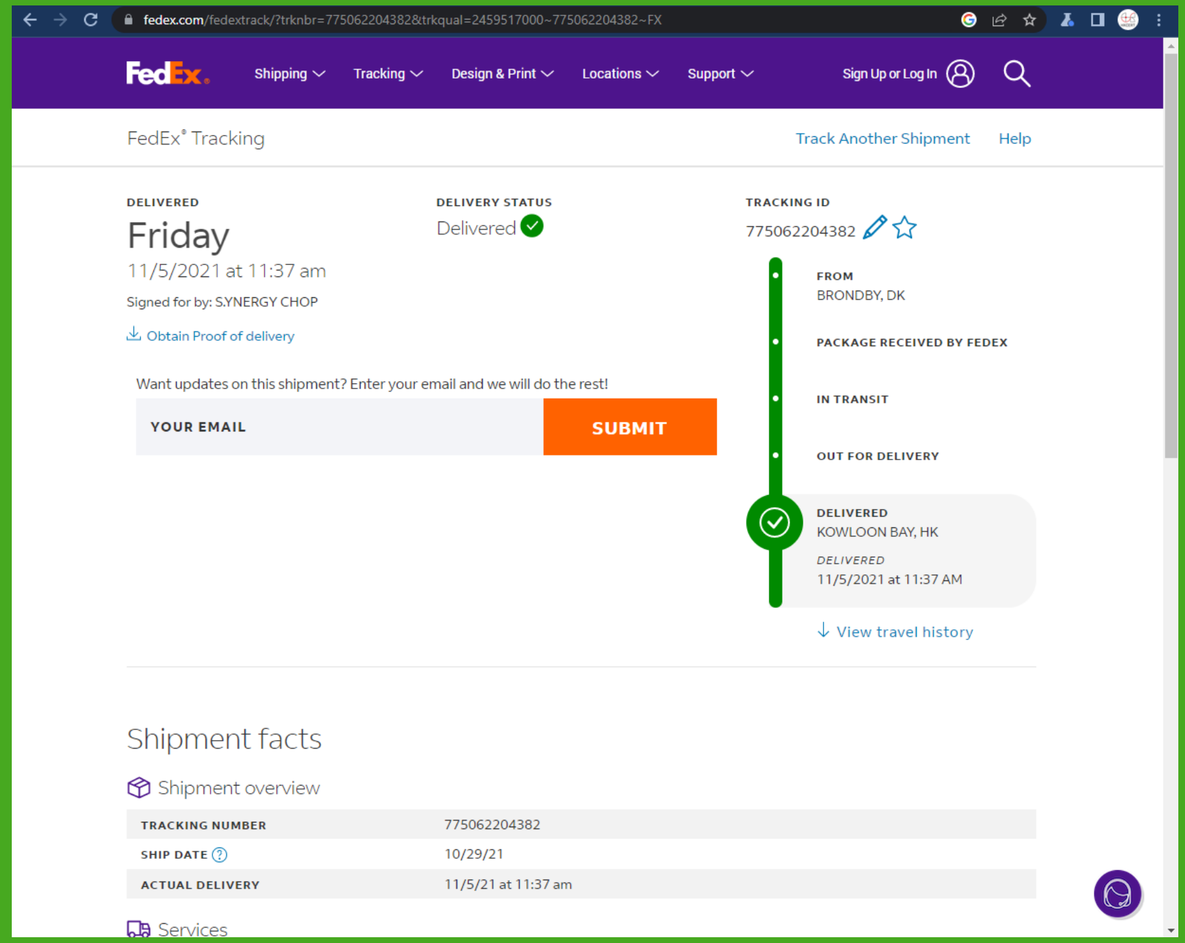




資料來源 Source: 香港網絡保安事故協調中心 (HKCERT)

意圖竊取個人 / 敏感資料





資料來源 Source: 香港網絡保安事故協調中心 (HKCERT)

保安貼士

檢查寄件者網域 — 學校官方通常是 @school.edu.hk

不要直接點郵件連結— 手動登入校網系統

不要回覆任何可疑的電郵或訊息，並立即刪除

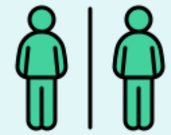
提交個人或敏感資訊時保持警惕

多管道查證 — 直接打電話給校務處或當面確認

技術防護與權限管理

開啟雙重驗證 (2FA) – Google / Microsoft / EDB Portal

公私帳號分離



避免校務帳號註冊外部網站

最小權限原則 – 僅給必要權限

如果你是 Google Workspace Admin 或 學校系統管理員：

- 隨時停用臨時帳號（代課、實習老師離職後）
- 定期檢視學生登入記錄
- 不開放多餘權限給學生
- 提醒學生不可利用學校帳號註冊遊戲或外部網站

「共建安全網絡」資訊保安推廣活動

推廣活動包括專題研討會、學校探訪、派發宣傳單張及海報、電台節目廣播，以及舉辦不同類型的比賽等。

資訊保安講座

為中小學和大專院校舉辦免費資訊保安講座，提升學生、教師及家長對網絡安全的認識。

涵蓋的主題包括：網絡欺凌、釣魚攻擊、人工智能/深度偽造騙案、事實查核、網絡禮儀、密碼管理

資安探訪團

每年與香港電台第二台合作製作「資安探訪團」。
節目探訪學校或非政府機構，由資安專家與港台DJ以輕鬆方法與學生分享網安訊息。

詳情及參加方法：

「共建安全網絡」資訊保安推廣活動

比賽

- 以有趣互動的方式提高公眾對網絡安全的認識

2026
三月

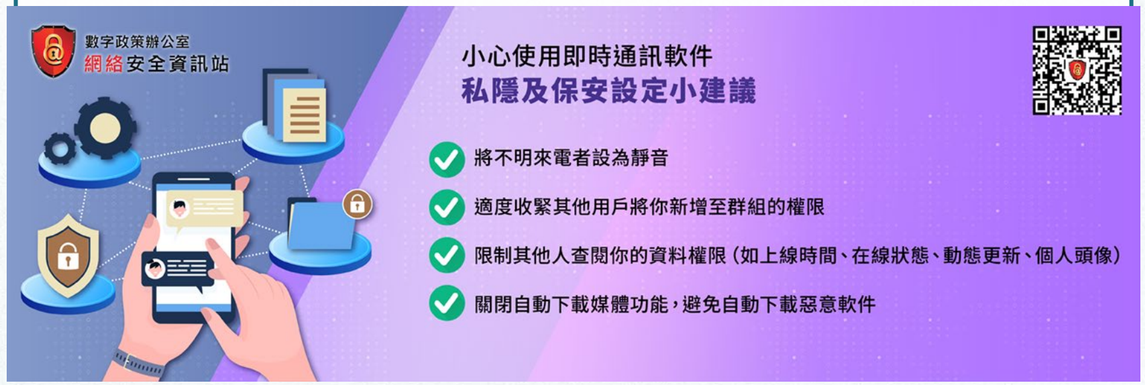
AI 四格漫畫生成比賽，設中學組、小學組及公開組，並設「最積極參與學校獎」，期望大家踴躍參與！

電台節目

- 每週於香港電台播放「E個世界至醒短訊」傳遞網安訊息
- 廣播內容同時上載於網絡安全資訊站供參考

RTHK 香港電台

網絡安全資訊站
www.cybersecurity.hk



參考資源

網絡安全資訊站由數字政策辦公室全力支援，
為一般用戶、學校及中小企提供實用的網安資訊與
最新活動消息。

「資源中心」載有網絡安全教育及宣傳資源，
如海報、單張及小冊子等，歡迎下載。

網絡安全資訊站
www.cybersecurity.hk

網絡安全資訊站

參考資源

Scameter+ 防騙視伏APP

HKCERT 香港網絡安全事故協調中心

THANK YOU