

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



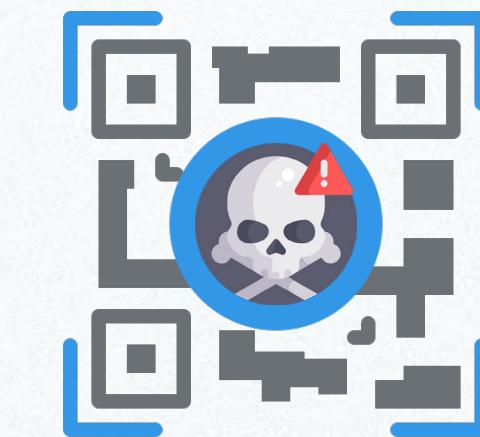
主題

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



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



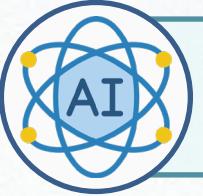
通常擁有校內系統存取權限



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。

Congratulations! 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

陌生寄件人或不明的電郵地址

1

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

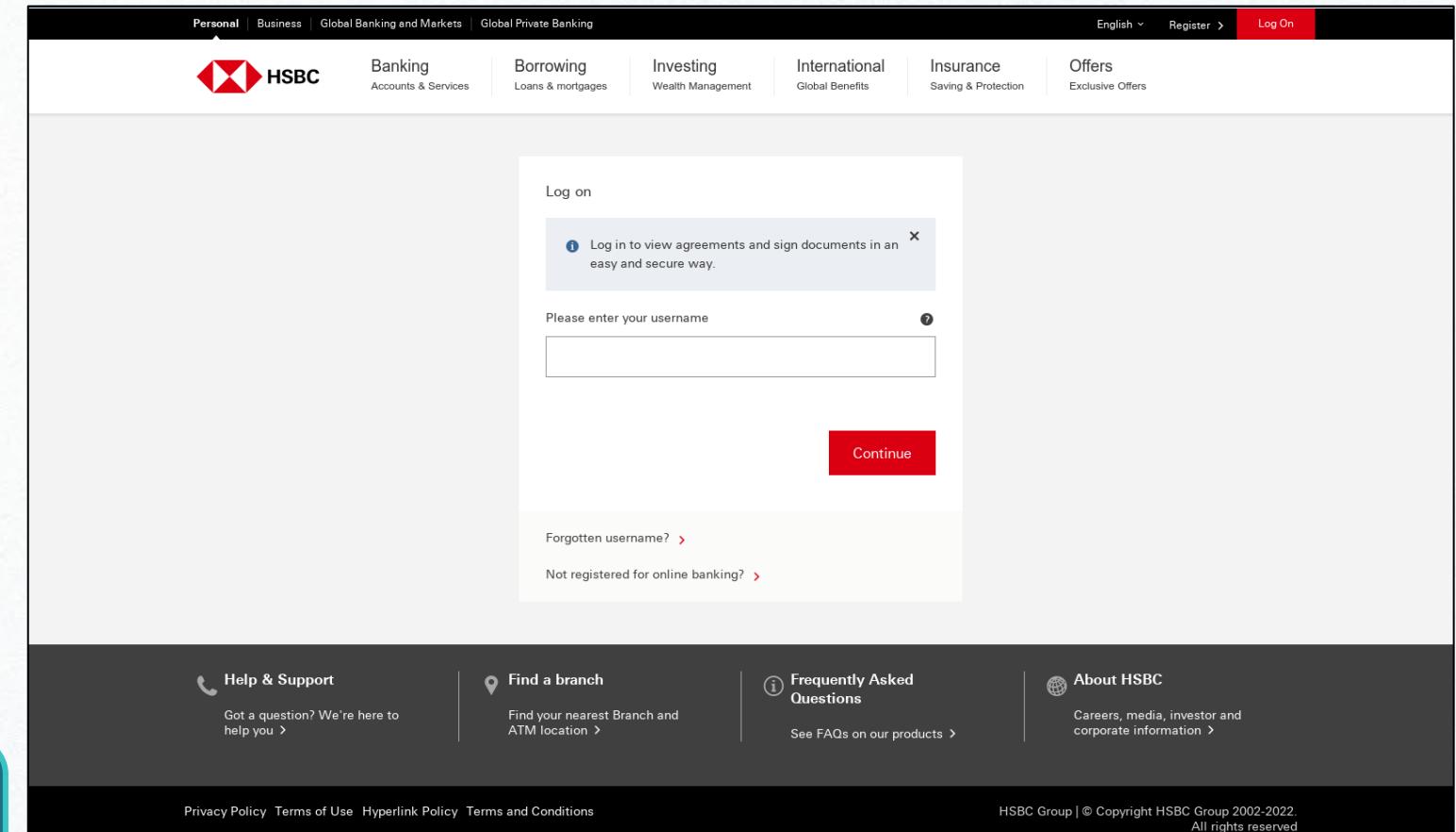
帶誤導性超連結

3

要求輸入個人 / 敏感資料

Phishing email

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



釣魚電郵例子



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

The image shows a screenshot of a SmarTone website's "Quick Claim Your Gift" page.

Page Headers:

- CONSUMER BUSINESS CARRIER & WHOLESALE
- FIND US ACCESSIBILITY QUICK PAY / RECHARGE
- SmarTone MOBILE PLANS DEVICES TV & INTERNET DIGITAL PRODUCTS
- SUPPORT MY ACCOUNT

Section Headers:

- Quick Claim Your Gift
- You can claim your gift card quickly with no login required.

Form Fields:

- YOUR SMARTONE ACCOUNT: Enter Your Mobile, Land line or Internet Number
- NEXT

釣魚短訊例子

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



A screenshot of the HSBC login page. The URL in the browser bar is `alfalahkita[.]com[/]mobile[/]key[/]login.php`. The page features the HSBC logo and navigation links for Personal, Business, Global Banking and Markets, and Global Private Banking. The main content area is titled "Log on" with a sub-instruction: "Log in to view agreements and sign documents in an easy and secure way." It includes fields for "Please enter your username" and a "Continue" button. Below the form are links for "Forgotten username?" and "Not registered for online banking?". The footer contains links for Help & Support, Find a branch, Frequently Asked Questions, and About HSBC. The copyright notice at the bottom states: "HSBC Group | © Copyright HSBC Group 2002-2022. All rights reserved".

釣魚網站的特徵

1 與真實網址相似
hxxps://www[.]bochk-cn[.]com/

2 複製真實網頁介面

https://www.bochk-cn.com/

Bank Of China (Hong Kong)

Home About Us Our Services Login/Sign Up Contact Online Login

Send us a Message info@bochk-cn.com

Opening Hours Mon - Sat: 7:00 - 18:00

The Strongest Bank in Hong Kong and Asia Pacific

THE ASIAN BANKER THE STRONGEST BANK IN HONG KONG AND ASIA PACIFIC 2022 by balance sheet

釣魚網站的特徵

https://www.acct.bochk-cn.com/s/online/

Bank Of China (Hong Kong)

中國銀行(香港)
BANK OF CHINA (HONG KONG)

Home Insurance Loans Credit cards Savings Travel

Select Language Translate

3 視覺設計不佳

4 意圖竊取個人 / 敏感資料

You are logged out

Login

Please enter your details below

Your username: Remember my username

Your password:

Need help with your login?
Forgotten your logon details

Login

Login timeout
To protect your personal information, your session will automatically timeout after 10 minutes of inactivity.

Can we help?

Just ask if you have a question about any aspect of Bank Of China (Hong Kong) Limited online banking.

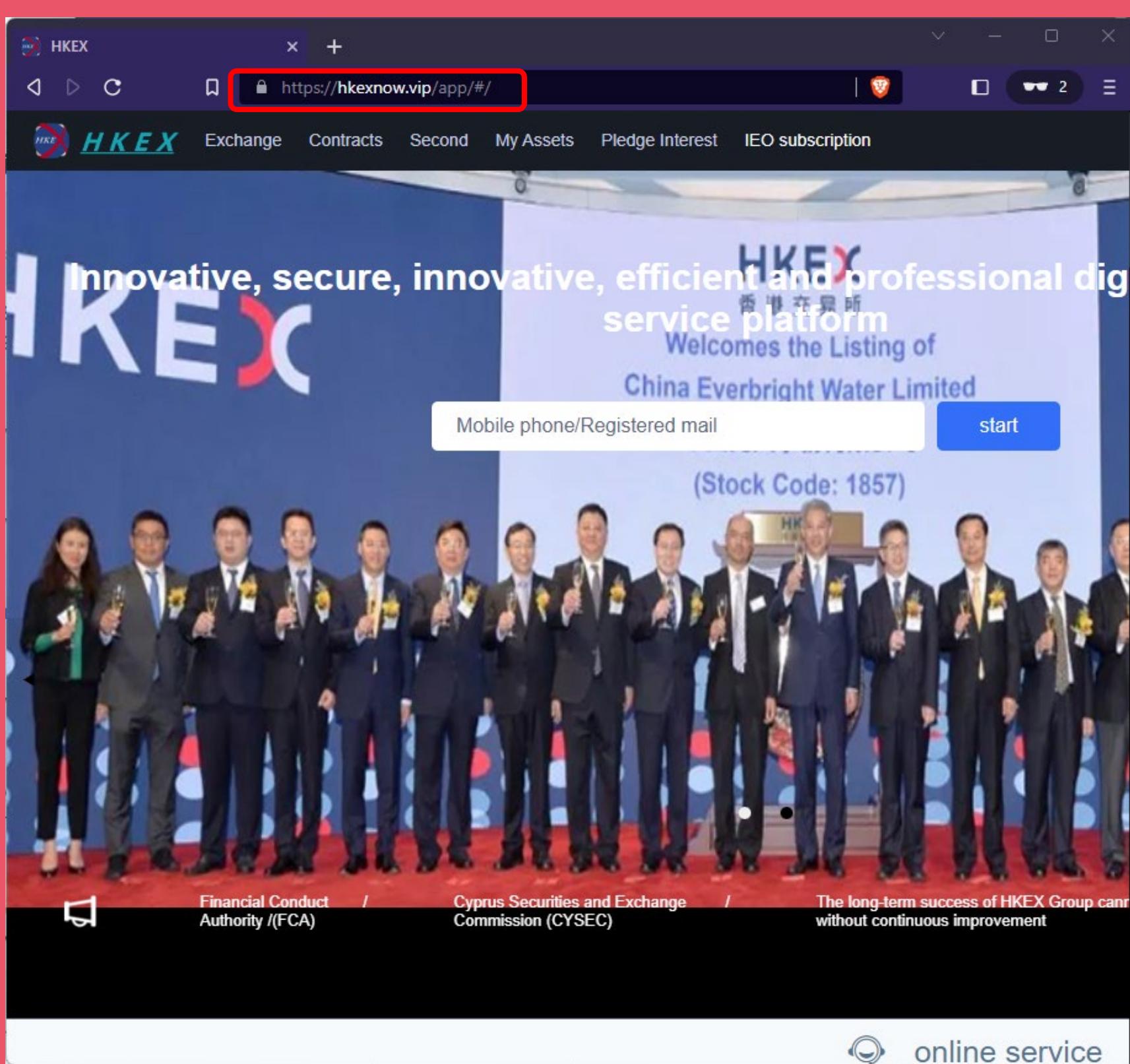
Online Support

Register, Activate or Re-set your account password.

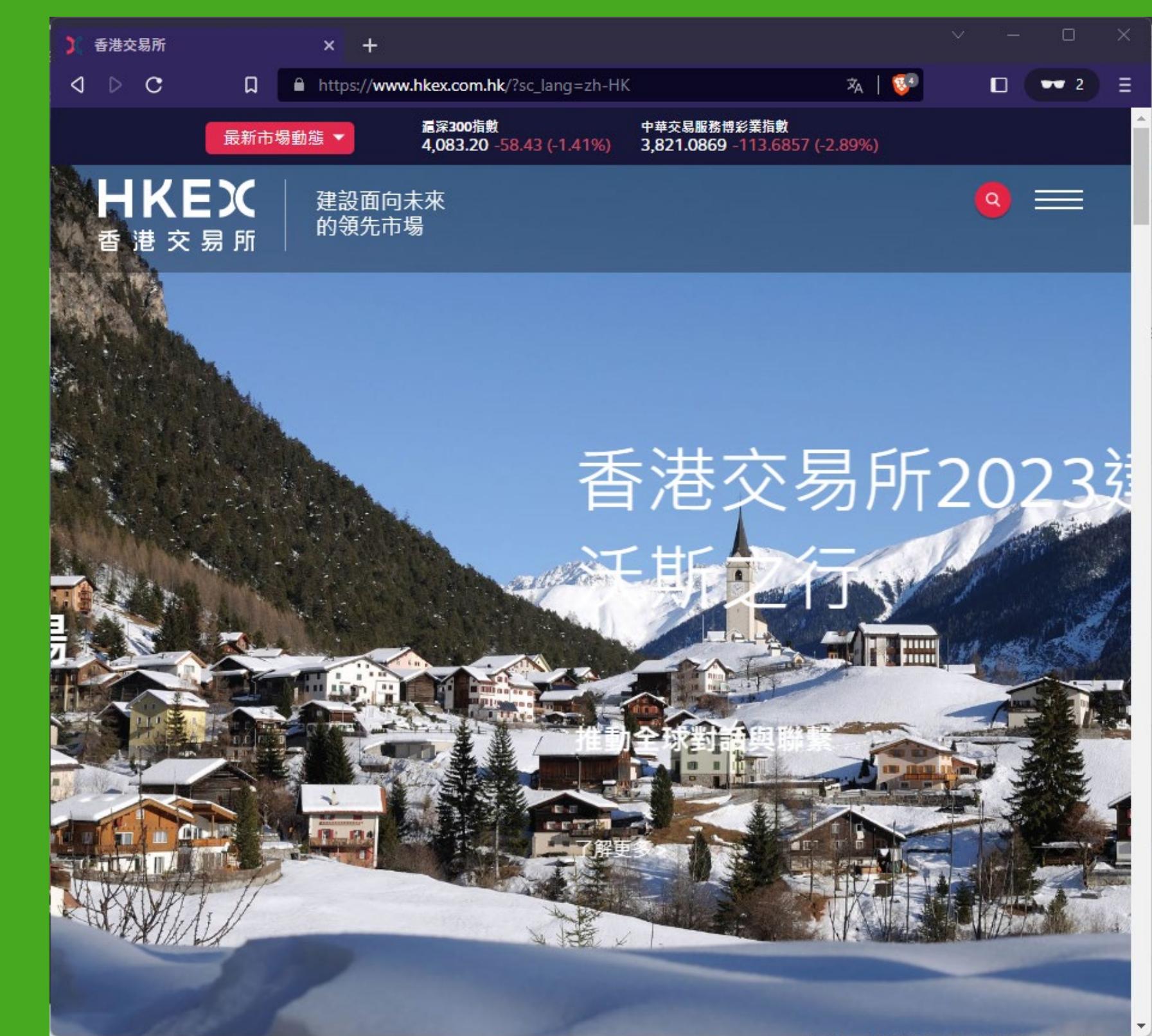
Register



與真實網址相似



A screenshot of a fake HKEX website. The URL in the address bar is <https://hkexnow.vip/app/#/>. The page features a large banner for China Everbright Water Limited's listing, a photo of a group of people in suits, and logos for FCA and CYSEC. A red box highlights the suspicious URL.



A screenshot of the real HKEX website at https://www.hkex.com.hk/?sc_lang=zh-HK. The page shows market data for the Hang Seng 300 Index and the Chinese Exchange Services Composite Index, along with a scenic snowy mountain landscape and a banner for the 2023 Swiss tour.

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



The screenshot shows a browser window with a red border. The URL in the address bar is <https://livraison.builderallwppro.com/de/net/login.php>. The page content is a仿冒的Netflix登录界面，包含“NETFLIX”标志、电影海报缩略图（如《Stranger Things》、《Cable Girls》）以及“Einloggen”按钮。输入框和按钮等元素与真实网站相似，但URL地址栏中的域名是伪造的。

The screenshot shows a browser window with a green border. The URL in the address bar is <https://www.netflix.com/hk-en/login>. The page content is the official Netflix login interface, featuring the “NETFLIX” logo, movie posters, and a “Sign In” button. The URL in the address bar is correct and matches the official Netflix domain.



視覺設計不佳

A screenshot of a web browser showing a fake iCloud login page. The page features a large red circle highlighting the entire form area, which includes input fields for Apple ID and Password, and a 'Keep me signed in' checkbox. Below the form is a 'Forgot Apple ID or password?' link. At the bottom, there are links for 'Create Apple ID', 'System Status', and 'Privacy Policy'. The URL in the address bar is https://www.apple.com-kor.cloud/find/.



A screenshot of the official iCloud login page. The page has a clean design with a green background. It features a large checkmark icon at the top right. Below it is the text 'Sign in with Apple ID'. There is an input field for 'Apple ID' with a right-pointing arrow button. A 'Keep me signed in' checkbox is located below the input field. At the bottom, there are links for 'Forgot Apple ID or password?' and 'Create Apple ID'.



意圖竊取個人 / 敏感資料



Dangerous | fedex-track.susl.live

FedEx. 🌐

FedEx® Tracking

DELIVERED Saturday 12/17/2022 at 19:8
Signed for by: S.YNERGY CHOP
Obtain Proof of delivery

DELIVERY STATUS Delay Delivery ⓘ
Get Status Updates

TRACKING ID 775062204382 🖊️ ⭐

PACKAGE RECEIVED BY FEDEX
IN TRANSIT
OUT FOR DELIVERY
ABNORMAL RETURN TO LOGISTICS CENTER
INCORRECT ADDRESS, DELAYED DELIVERY
12/17/2022 AT 19:8

Shipment facts

Verify Billing Address
The delivery address is wrong, please update the correct delivery address as soon as possible to restore the package status

Full name Street Address 2 (OPT)

Street Address 1

City Select State ZIP Code™ (OPT)

Phone Number

fedex.com/fedextrack/?trknbr=775062204382&trkqual=2459517000~775062204382~FX

FedEx. Shipping Tracking Design & Print Locations Support Sign Up or Log In 🌐

FedEx® Tracking

DELIVERED Friday 11/5/2021 at 11:37 am
Signed for by: S.YNERGY CHOP
Obtain Proof of delivery

DELIVERY STATUS Delivered ⓘ

Want updates on this shipment? Enter your email and we will do the rest!

YOUR EMAIL SUBMIT

TRACKING ID 775062204382 🖊️ ⭐

FROM BRONDBY, DK
PACKAGE RECEIVED BY FEDEX
IN TRANSIT
OUT FOR DELIVERY
DELIVERED KOWLOON BAY, HK
DELIVERED 11/5/2021 at 11:37 AM

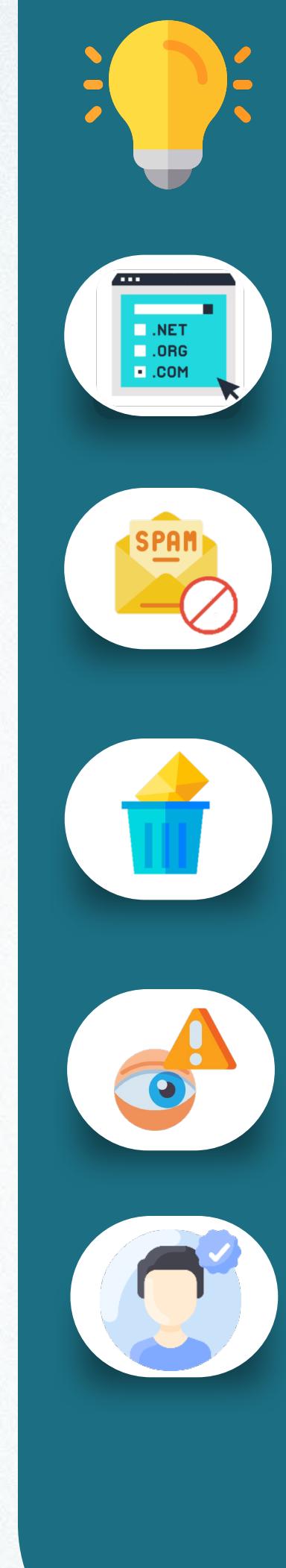
View travel history

Shipment facts

Shipment overview

TRACKING NUMBER	775062204382
SHIP DATE ⓘ	10/29/21
ACTUAL DELIVERY	11/5/21 at 11:37 am

Services



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

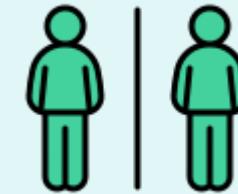


開啟雙重驗證 (2FA) –
Google / Microsoft /
EDB Portal

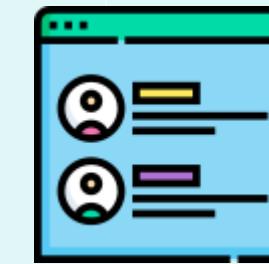


避免校務帳號
註冊外部網站

公私帳號分離



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

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！



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。



學習天地

主頁 > 學習天地

安全使用視像會議指南

視像會議逐漸成為有效的通訊方式，可方便遙距工作，以及讓位處不同地點的用戶進行實時溝通。這項技術為我們帶來很多便利，但同時也存在一些風險和挑戰。

開始課程

遙距工作的保安

鑑於近期冠狀病毒爆發，不少機構安排員工遙距工作，減少社交接觸。

開始課程

深度偽造

風險與應對

「深度偽造」一詞由「深度學習」與「偽造」結合而成，是指利用人工智能技術，將一個人的臉容或聲音合成至特定圖像、影片或音頻中，從而創造出看似真實的偽造內容。

甚麼是深度偽造？

深度偽造的惡意用途

辨識及應對深度偽造

識別環痕：細心留意圖像、影片或音頻是否有不自然的動作、不協調或不合常規的地方。

評估來源：衡量發布內容的媒體的可信度。

進行事實查核：對收到的內容抱持合理的懷疑態度，並透過可靠的途徑查核內容是否屬實。

勒索：冒充受害者的親友、工作夥伴或其他可信賴人士，從而騙取金錢。

誣言：捏造對受害者造成負面影響的內容，藉威脅公開內容以敲詐受害者。

網絡欺凌：製作冒犯或滋擾受害者的惡意內容，並於網絡上發布。

保護個人資料：切勿隨意公開個人資料，以免被利用來生成深度偽造內容。

虛假資訊：製作假新聞故意誤導公眾或影響輿論。



網絡安全資訊站
www.cybersecurity.hk

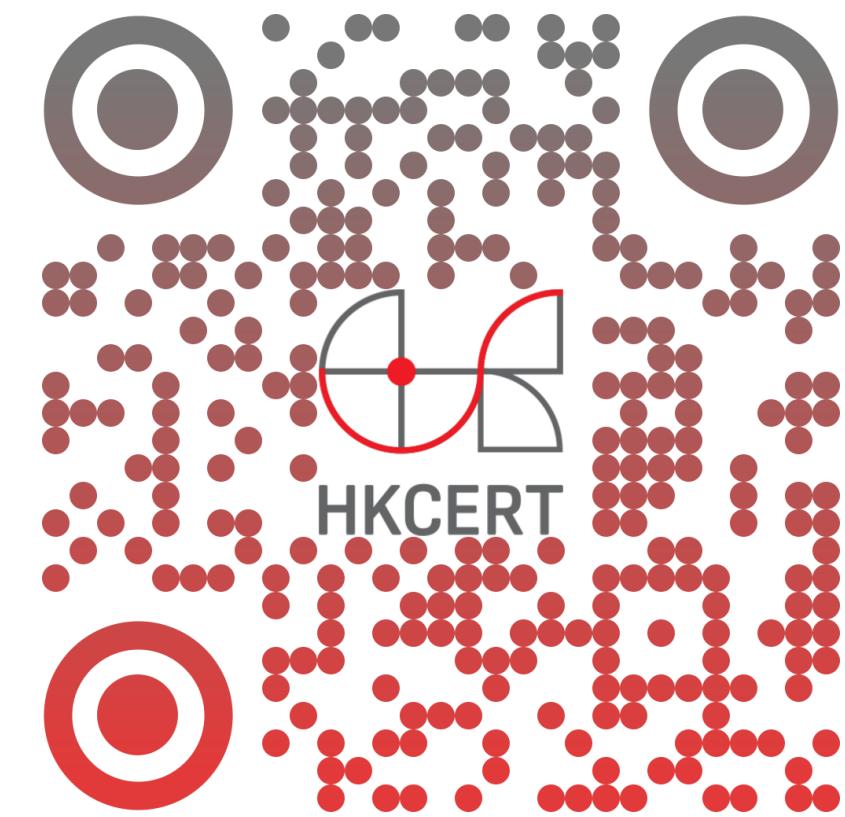


Q 網絡安全資訊站

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