IT&HI

Managing the Latest Cybersecurity Landscape in Healthcare Sector
透視醫療保健網絡安全新形勢

Fuller Yu

Chief of IT Operations, Hospital Authority
Co-Chair of Cyber Security Work Stream, Global Digital Health Partnership

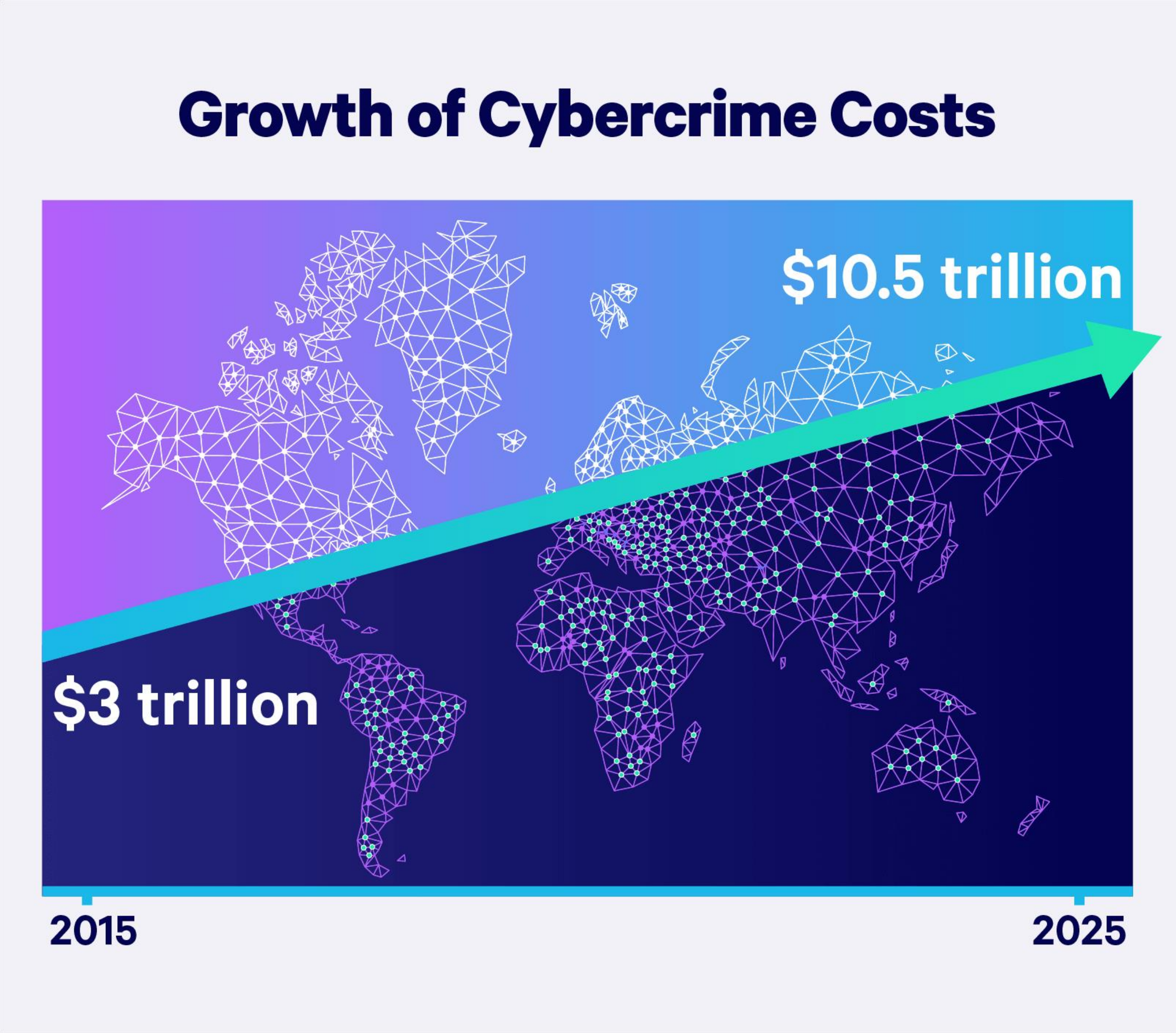
October 2024

The Cyber Landscape in 2024

What we saw in 2024

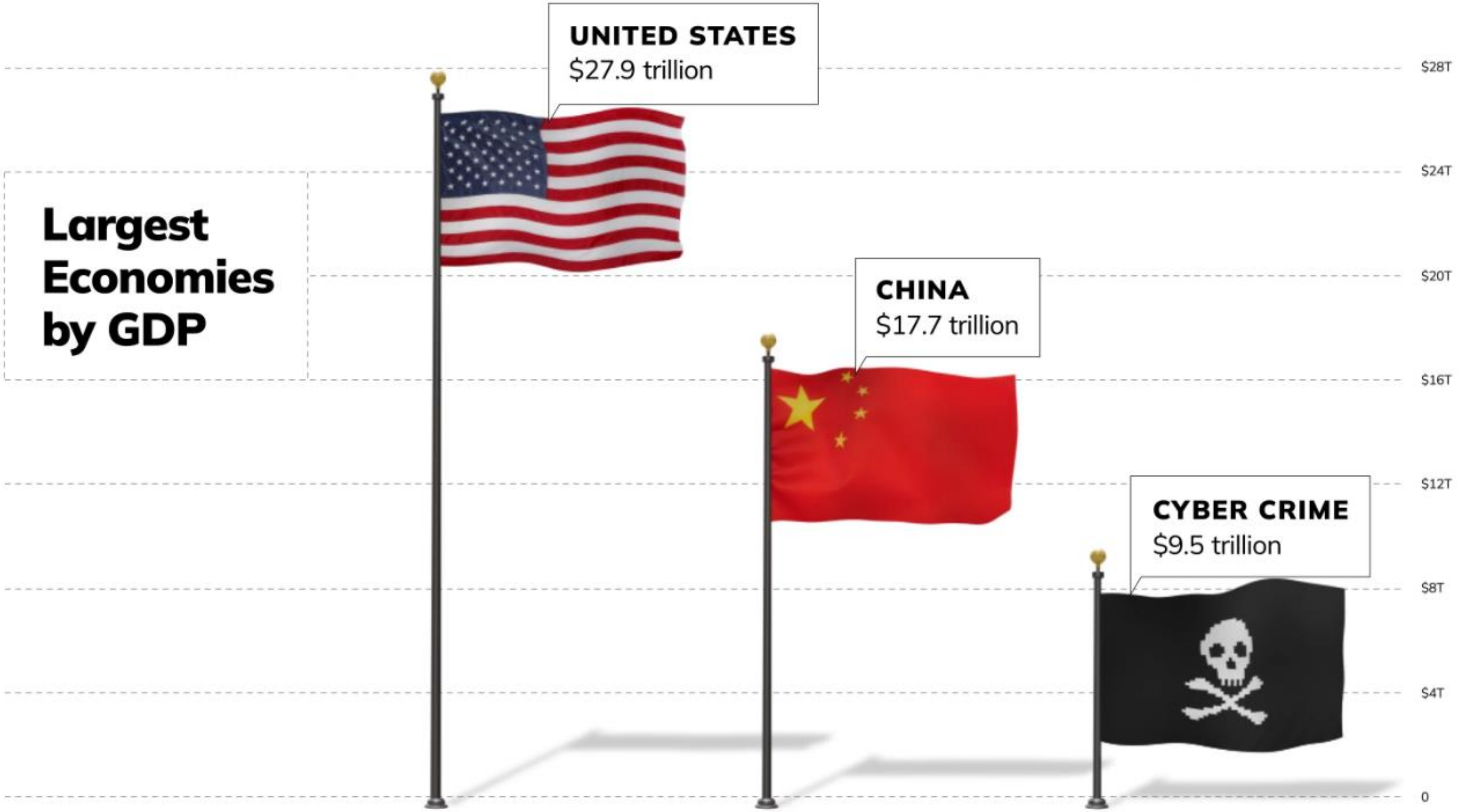
- ⚠ Cybercrime to cost the world $10.5 Trillion annually by 2025
- ⚠ Average cost of a data breach in healthcare sector is US$10m
- ⚠ Hong Kong is an attractive cyberattack target
- ⚠ Ransomware attacks target all companies from enterprise to SME
- ⚠ Insecure remote access and uninformed end users are still root cause

Cybercrime to cost the world $10.5 Trillion annually by 2025



Source: Cybersecurity Ventures

Cybercrime is the Third Largest Economy just after USA and China



Source: IMF, Bloomberg, Cybersecurity Ventures

Average Cost of a Data Breach of Healthcare Sector is US$10m

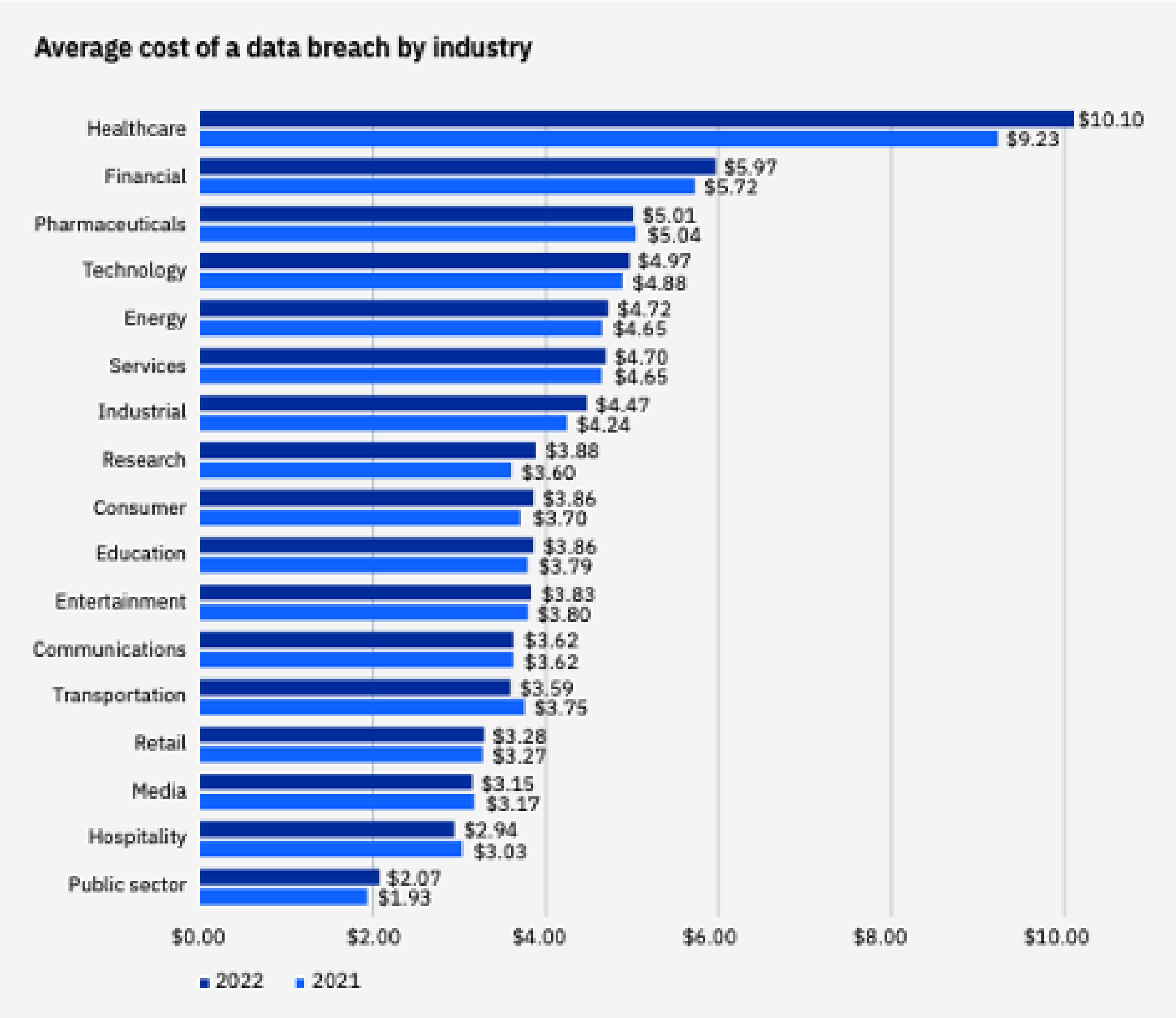


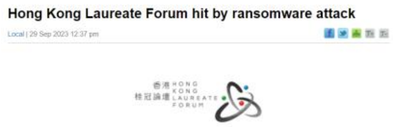
Figure 4: Measured in USD millions

Source: IBM

Hong Kong is an Attractive Cyberattack Target

Cyberport
Aug-2023

Sep-2023
Consumer Council


Hong Kong Laureate Forum hit by ransomware attack
Local | 29 Sep 2023 12:37 pm

HK Laureate Forum
Sep-2023

Oct-2023
HK Ballet

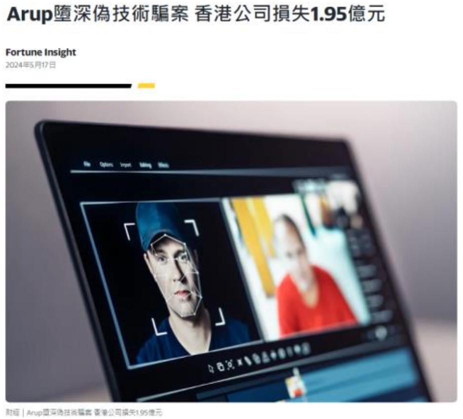
HK Post
Oct-2023

Feb-2024
HKCT
(港專)

仁安醫院
UNION HOSPITAL

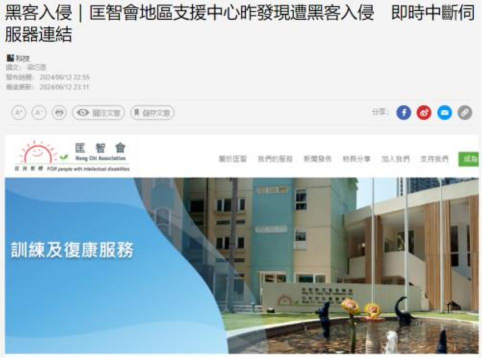
Union Hospital
Apr-2024

May-2024
ARUP


Arup墮深偽技術騙案 香港公司損失1.95億元

Fortune Insight
2024年5月17日

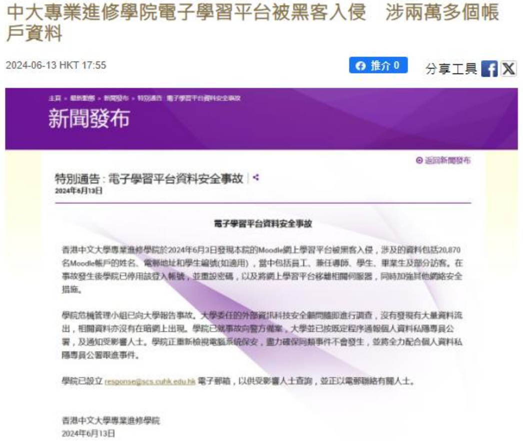
財經 | Arup墮深偽技術騙案 香港公司損失1.95億元


黑客入侵｜匡智會地區支援中心昨發現遭黑客入侵　即時中斷伺服器連結

科技
撰文： [illegible]
發佈時間： 2024/06/12 22:55
最後更新： 2024/06/12 23:11

匡智會
May-2024

Jun-2024
中大專業
進修學院


中大專業進修學院電子學習平台被黑客入侵　涉兩萬多個帳戶資料

2024-06-13 HKT 17:55

推介 0
分享工具
主頁 » 最新動態 » 新聞發布 » 特別通告：電子學習平台資料安全事故
新聞發布
返回新聞發布

特別通告：電子學習平台資料安全事故
2024年6月13日

電子學習平台資料安全事故

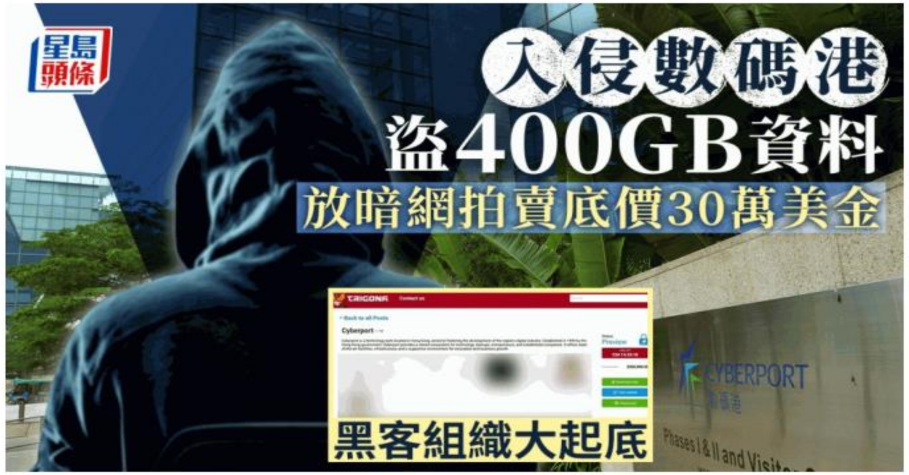
香港中文大學專業進修學院於2024年6月3日發現本院的Moodle網上學習平台被黑客入侵，涉及的資料包括20,870名Moodle帳戶的姓名、電郵地址和學生編號(如適用)，當中包括員工、兼任導師、學生、畢業生及部分訪客。在事故發生後學院已停用該登入帳號，並重設密碼，以及將網上學習平台移離相關伺服器，同時加強其他網絡安全措施。

學院危機管理小組已向大學報告事故。大學委任的外部資訊科技安全顧問隨即進行調查，沒有發現有大量資料流出，相關資料亦沒有在暗網上出現。學院已就事故向警方備案，大學並已按既定程序通報個人資料私隱專員公署，及通知受影響人士。學院正重新檢視電腦系統保安，盡力確保同類事件不會發生，並將全力配合個人資料私隱專員公署跟進事件。

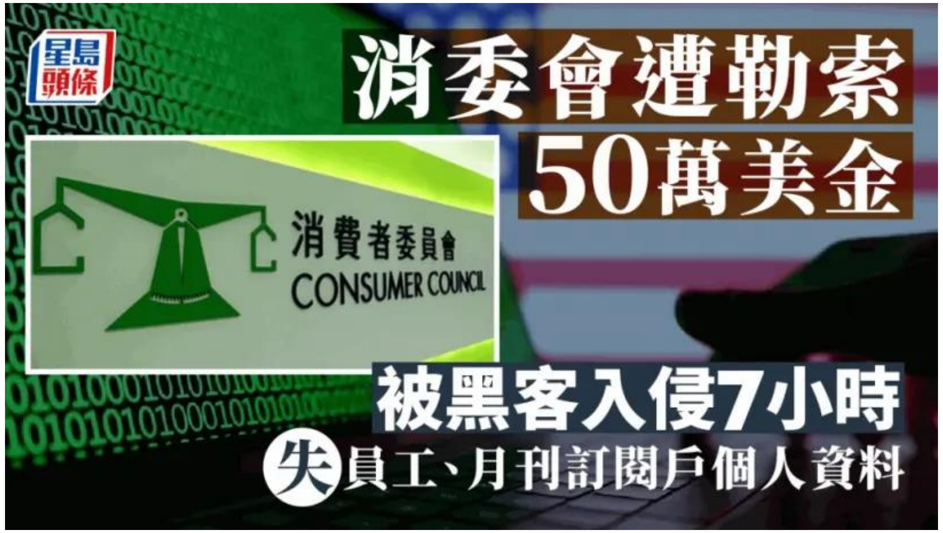
學院已設立 response@scs.cuhk.edu.hk 電子郵箱，以供受影響人士查詢，並正以電郵聯絡有關人士。

香港中文大學專業進修學院
2024年6月13日

And the consequences are significant for both companies and their customers



數碼港昨日(6日)公布發現一宗網絡安全事件，涉及未經授權的第三方入侵數碼港部分的電腦系統。



消委會電腦系統遭黑客入侵，於今早(22日)10時召開記者會交代詳情。陳浩元攝

醫療服務行業的網絡安全威脅與挑戰

People

- 醫療服務員工的網絡安全能力較低
- 缺乏網絡安全人才以確保系統安全

Process

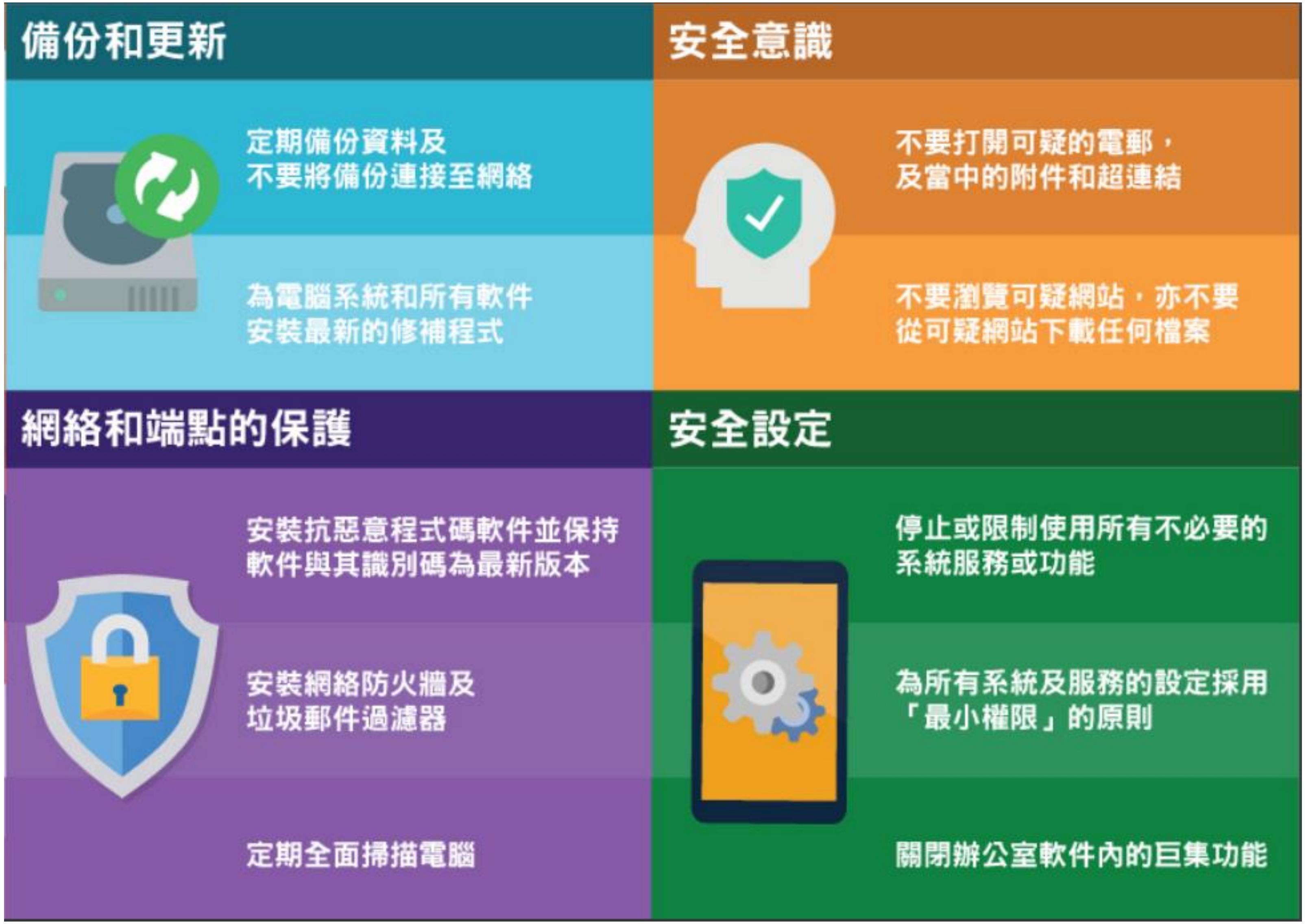
- 高價值醫療數據成為網絡罪犯目標
- 臨床系統變得重要，成為勒索軟件攻擊對象

Technology

- 對醫療設備和老舊系統的控制不足
- 新興技術帶來新的風險

ARE
YOU
READY?

Get the Basic Right to Avoid Being Low Hanging Fruit



備份和更新

定期備份資料及
不要將備份連接至網絡

為電腦系統和所有軟件
安裝最新的修補程式

安全意識

不要打開可疑的電郵，
及當中的附件和超連結

不要瀏覽可疑網站，亦不要
從可疑網站下載任何檔案

網絡和端點的保護

安裝抗惡意程式碼軟件並保持
軟件與其識別碼為最新版本

安裝網絡防火牆及
垃圾郵件過濾器

定期全面掃描電腦

安全設定

停止或限制使用所有不必要的
系統服務或功能

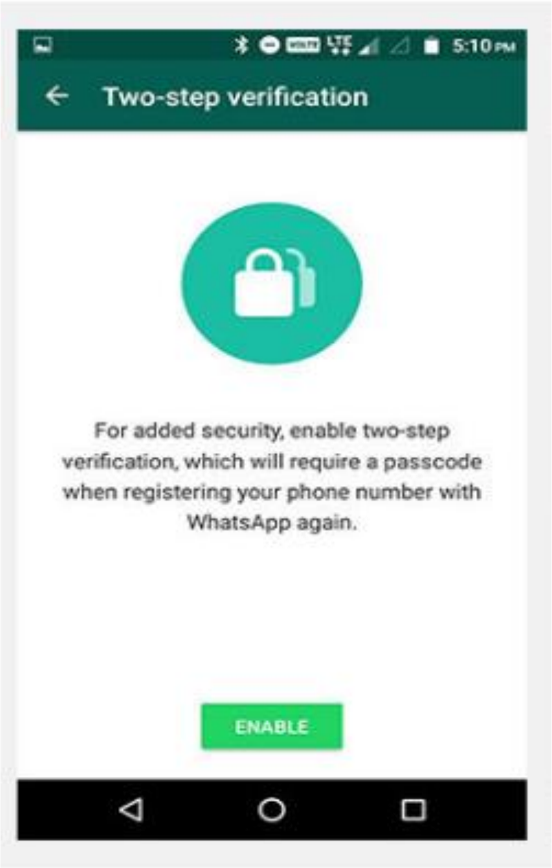
為所有系統及服務的設定採用
「最小權限」的原則

關閉辦公室軟件內的巨集功能

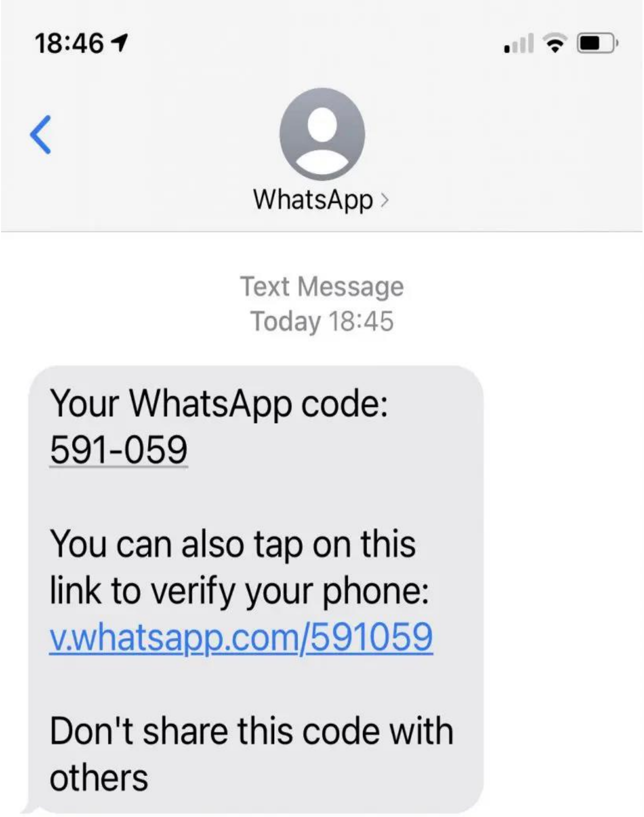
Source: HKCert.org

Enable 2-Factor Authentication

… and never disclose your OTP to anyone!



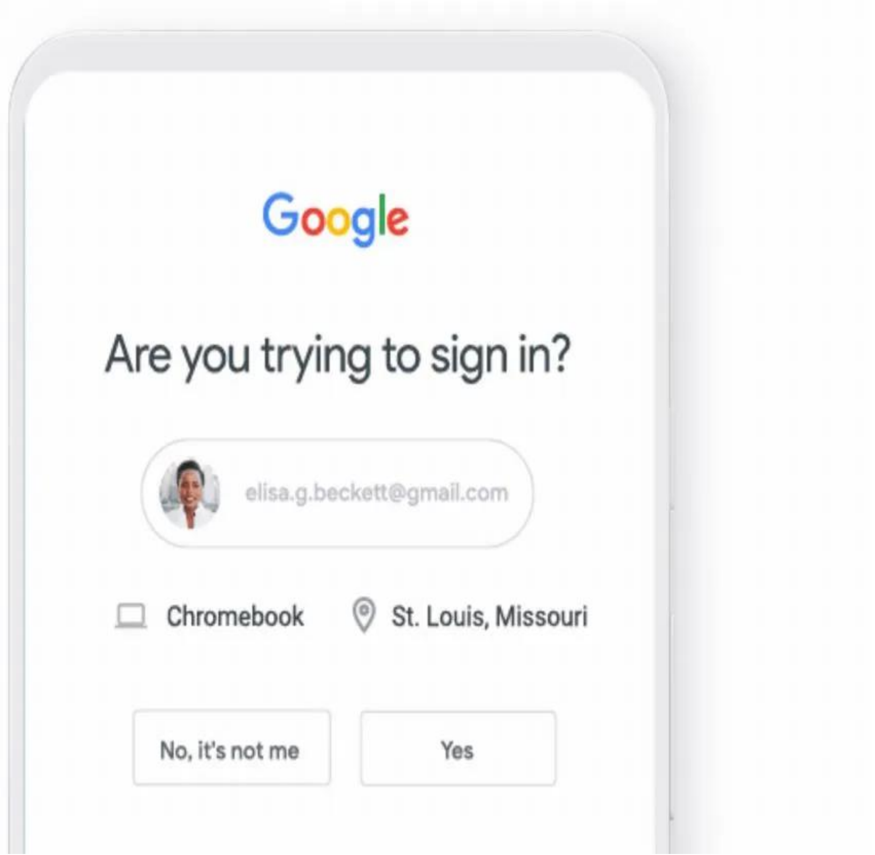
For added security, enable two-step verification, which will require a passcode when registering your phone number with WhatsApp again.



Your WhatsApp code: 591-059

You can also tap on this link to verify your phone: v.whatsapp.com/591059

Don't share this code with others



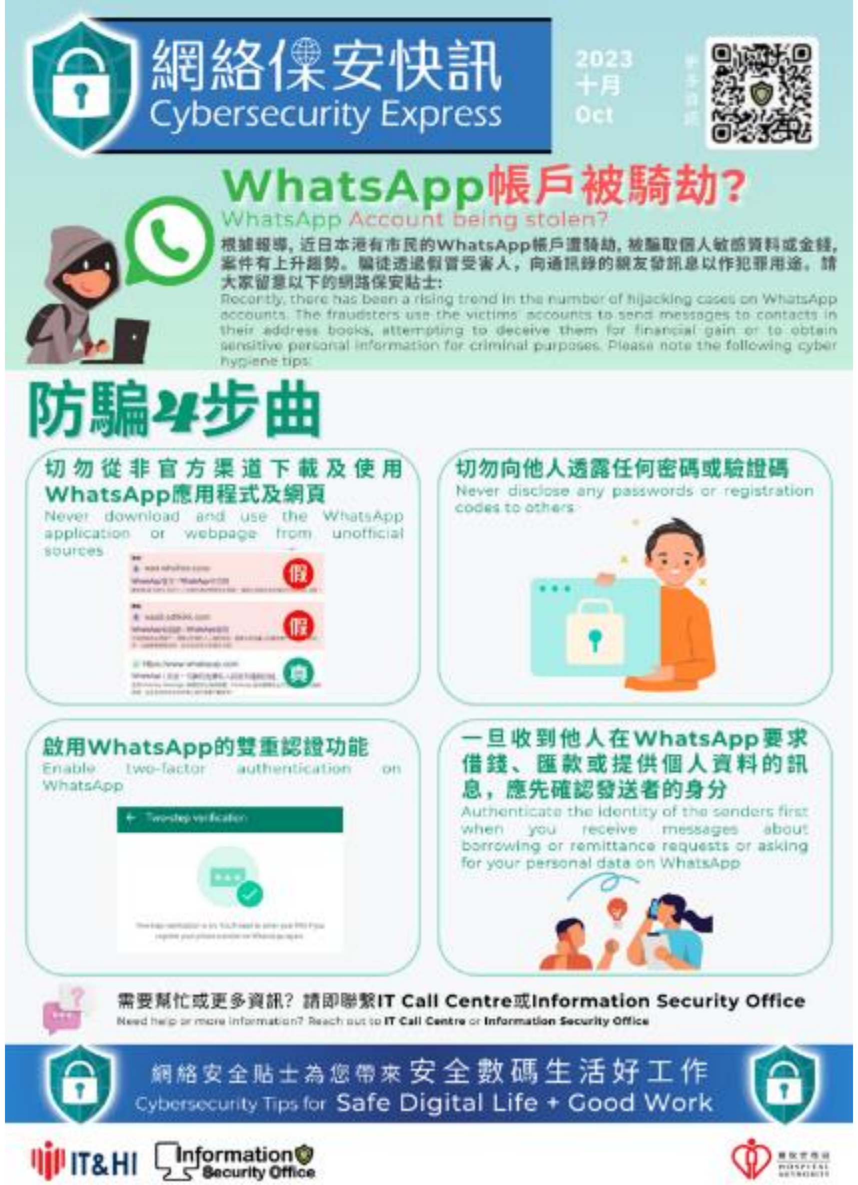
Are you trying to sign in?

elisa.g.beckett@gmail.com

Chromebook · St. Louis, Missouri

OTP is One Time Passcode

Scams are Anywhere so Need to be Always Vigilant!



網絡保安快訊
Cybersecurity Express

2023
十月
Oct

更多資訊

WhatsApp帳戶被騎劫?

WhatsApp Account being stolen?

根據報導，近日本港有市民的WhatsApp帳戶遭騎劫，被騙取個人敏感資料或金錢，案件有上升趨勢。騙徒透過假冒受害人，向通訊錄的親友發訊息以作犯罪用途。請大家留意以下的網絡保安貼士:

Recently, there has been a rising trend in the number of hijacking cases on WhatsApp accounts. The fraudsters use the victims' accounts to send messages to contacts in their address books, attempting to deceive them for financial gain or to obtain sensitive personal information for criminal purposes. Please note the following cyber hygiene tips:

防騙4步曲

切勿從非官方渠道下載及使用WhatsApp應用程式及網頁

Never download and use the WhatsApp application or webpage from unofficial sources

切勿向他人透露任何密碼或驗證碼

Never disclose any passwords or registration codes to others

啟用WhatsApp的雙重認證功能

Enable two-factor authentication on WhatsApp

一旦收到他人在WhatsApp要求借錢、匯款或提供個人資料的訊息，應先確認發送者的身分

Authenticate the identity of the senders first when you receive messages about borrowing or remittance requests or asking for your personal data on WhatsApp

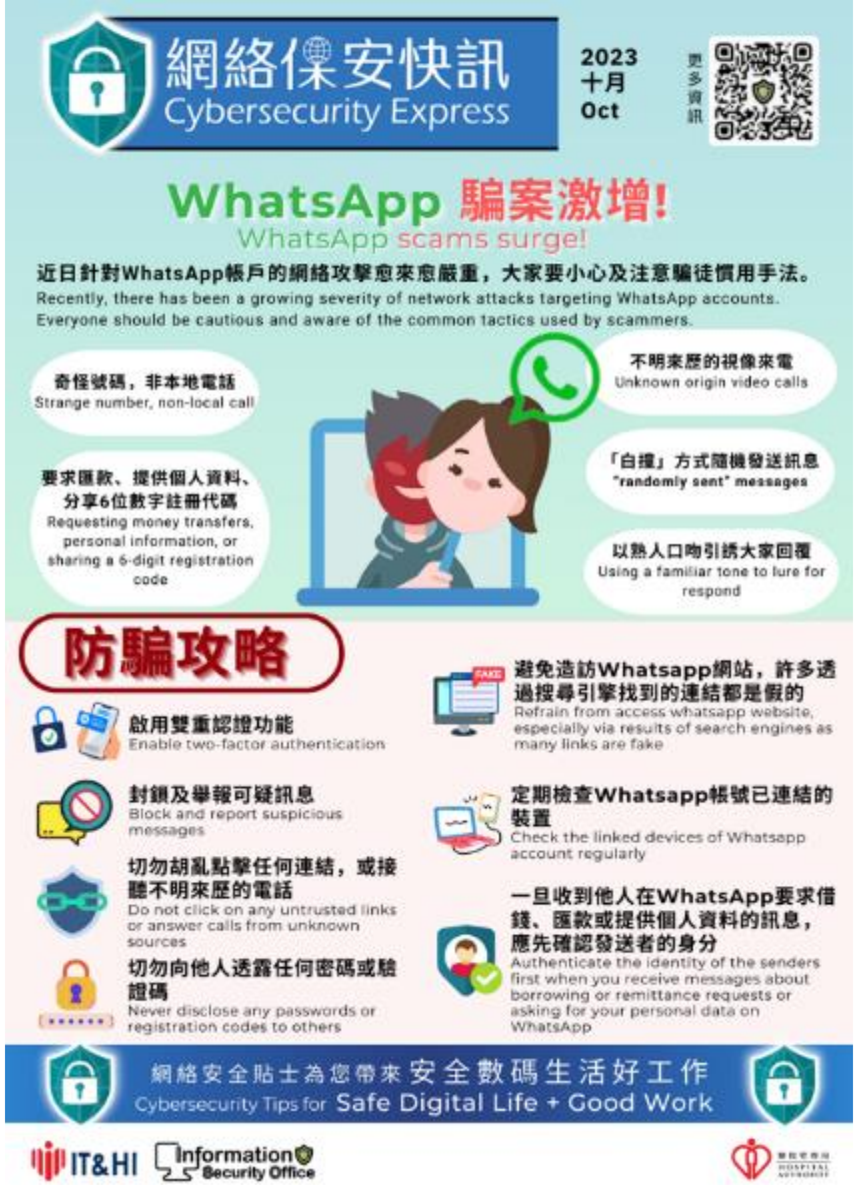
需要幫忙或更多資訊? 請即聯繫IT Call Centre或Information Security Office

Need help or more information? Reach out to **IT Call Centre** or **Information Security Office**

網絡安全貼士為您帶來 安全數碼生活好工作

Cybersecurity Tips for Safe Digital Life + Good Work

IT&HI Information Security Office



網絡保安快訊
Cybersecurity Express

2023
十月
Oct

更多資訊

WhatsApp 騙案激增!

WhatsApp scams surge!

近日針對WhatsApp帳戶的網絡攻擊愈來愈嚴重，大家要小心及注意騙徒慣用手法。

Recently, there has been a growing severity of network attacks targeting WhatsApp accounts. Everyone should be cautious and aware of the common tactics used by scammers.

奇怪號碼，非本地電話
Strange number, non-local call

要求匯款、提供個人資料、分享6位數字註冊代碼
Requesting money transfers, personal information, or sharing a 6-digit registration code

不明來歷的視像來電
Unknown origin video calls

「自撞」方式隨機發送訊息
"randomly sent" messages

以熟人口吻引誘大家回覆
Using a familiar tone to lure for respond

防騙攻略

啟用雙重認證功能
Enable two-factor authentication

封鎖及舉報可疑訊息
Block and report suspicious messages

切勿胡亂點擊任何連結，或接聽不明來歷的電話
Do not click on any untrusted links or answer calls from unknown sources

切勿向他人透露任何密碼或驗證碼
Never disclose any passwords or registration codes to others

避免造訪Whatsapp網站，許多透過搜尋引擎找到的連結都是假的
Refrain from access whatsapp website, especially via results of search engines as many links are fake

定期檢查Whatsapp帳號已連結的裝置
Check the linked devices of Whatsapp account regularly

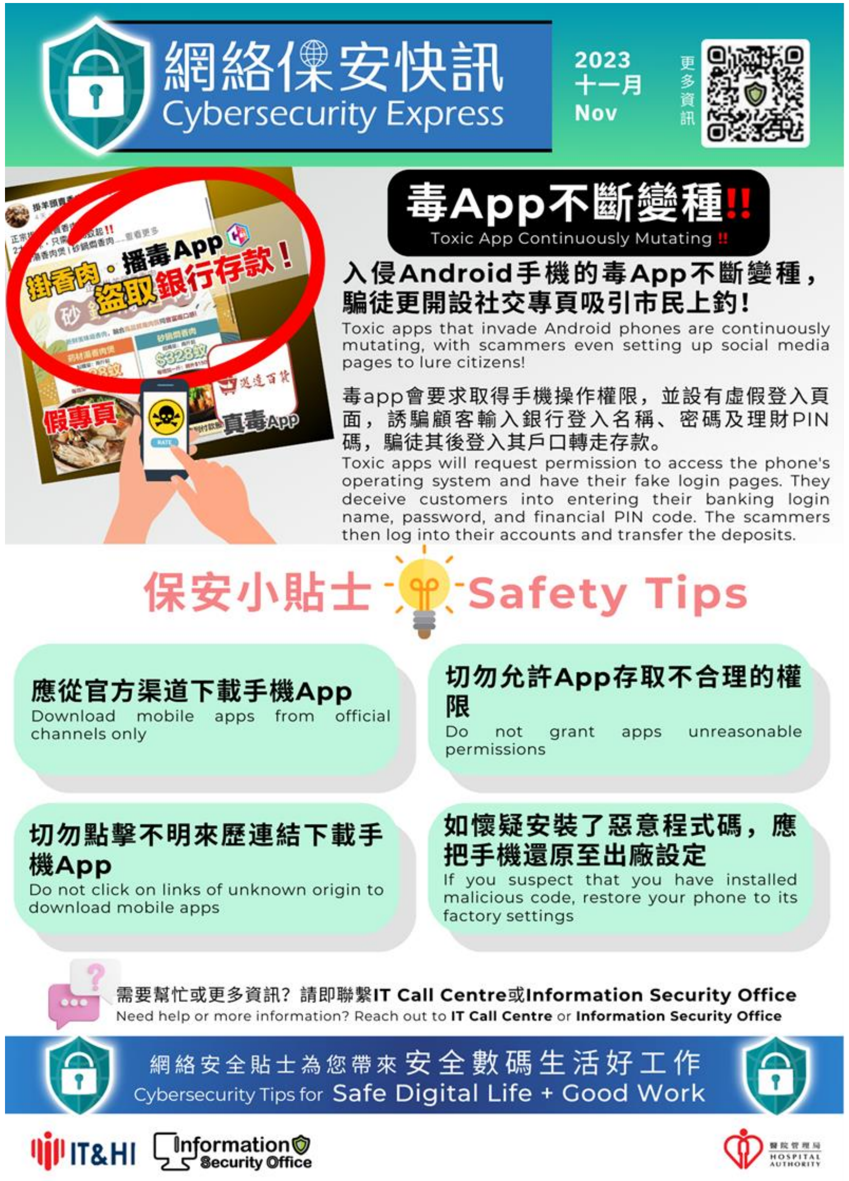
一旦收到他人在WhatsApp要求借錢、匯款或提供個人資料的訊息，應先確認發送者的身分
Authenticate the identity of the senders first when you receive messages about borrowing or remittance requests or asking for your personal data on WhatsApp

網絡安全貼士為您帶來 安全數碼生活好工作

Cybersecurity Tips for Safe Digital Life + Good Work

IT&HI Information Security Office

Scams are Anywhere so Need to be Always Vigilant!



網絡保安快訊 Cybersecurity Express

2023 十一月 Nov

更多資訊

毒App不斷變種!!

Toxic App Continuously Mutating !!

掛香肉・播毒App 盜取銀行存款！
假專頁
真毒App

入侵Android手機的毒App不斷變種，騙徒更開設社交專頁吸引市民上釣！

Toxic apps that invade Android phones are continuously mutating, with scammers even setting up social media pages to lure citizens!

毒app會要求取得手機操作權限，並設有虛假登入頁面，誘騙顧客輸入銀行登入名稱、密碼及理財PIN碼，騙徒其後登入其戶口轉走存款。

Toxic apps will request permission to access the phone's operating system and have their fake login pages. They deceive customers into entering their banking login name, password, and financial PIN code. The scammers then log into their accounts and transfer the deposits.

保安小貼士 Safety Tips

應從官方渠道下載手機App
Download mobile apps from official channels only

切勿允許App存取不合理的權限
Do not grant apps unreasonable permissions

切勿點擊不明來歷連結下載手機App
Do not click on links of unknown origin to download mobile apps

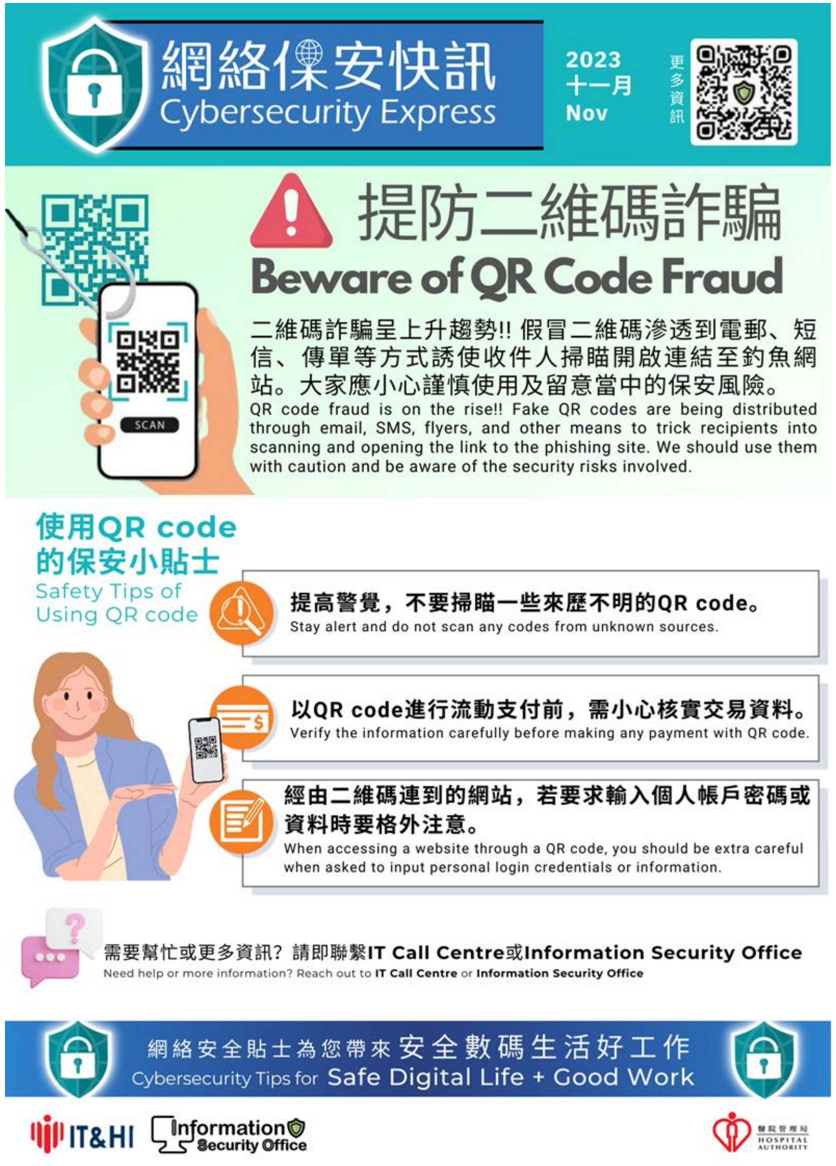
如懷疑安裝了惡意程式碼，應把手機還原至出廠設定
If you suspect that you have installed malicious code, restore your phone to its factory settings

需要幫忙或更多資訊？請即聯繫IT Call Centre或Information Security Office
Need help or more information? Reach out to **IT Call Centre** or **Information Security Office**

網絡安全貼士為您帶來安全數碼生活好工作
Cybersecurity Tips for Safe Digital Life + Good Work

IT&HI Information Security Office

醫院管理局 HOSPITAL AUTHORITY



網絡保安快訊 Cybersecurity Express

2023 十一月 Nov

更多資訊

提防二維碼詐騙 Beware of QR Code Fraud

二維碼詐騙呈上升趨勢!! 假冒二維碼滲透到電郵、短信、傳單等方式誘使收件人掃瞄開啟連結至釣魚網站。大家應小心謹慎使用及留意當中的保安風險。

QR code fraud is on the rise!! Fake QR codes are being distributed through email, SMS, flyers, and other means to trick recipients into scanning and opening the link to the phishing site. We should use them with caution and be aware of the security risks involved.

使用QR code的保安小貼士 Safety Tips of Using QR code

提高警覺，不要掃瞄一些來歷不明的QR code。
Stay alert and do not scan any codes from unknown sources.

以QR code進行流動支付前，需小心核實交易資料。
Verify the information carefully before making any payment with QR code.

經由二維碼連到的網站，若要求輸入個人帳戶密碼或資料時要格外注意。
When accessing a website through a QR code, you should be extra careful when asked to input personal login credentials or information.

需要幫忙或更多資訊？請即聯繫IT Call Centre或Information Security Office
Need help or more information? Reach out to **IT Call Centre** or **Information Security Office**

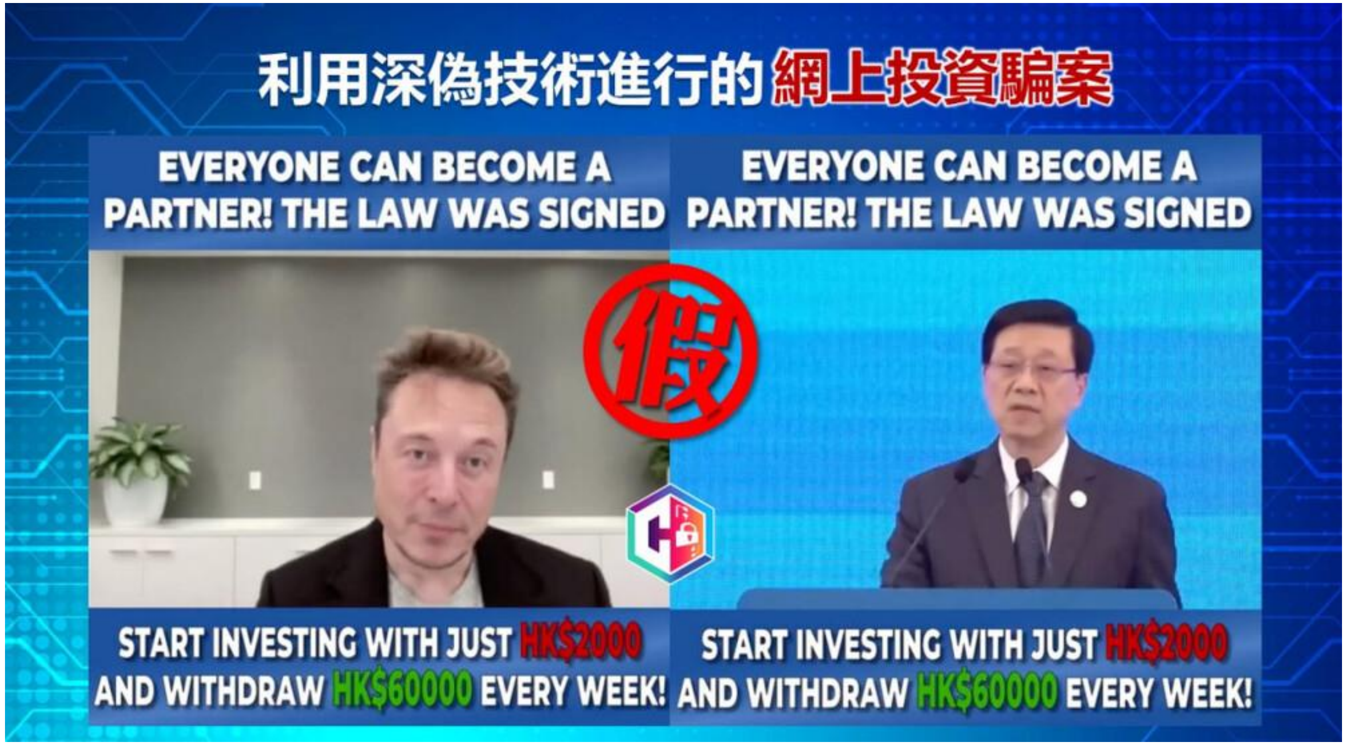
網絡安全貼士為您帶來安全數碼生活好工作
Cybersecurity Tips for Safe Digital Life + Good Work

IT&HI Information Security Office

醫院管理局 HOSPITAL AUTHORITY

Deep fake video call

- The first deepfake video conference scam in HK in Jan 2024
- Fraudster impersonated the victim's boss and swindled HK$200 million
- An employee of a multinational company was asked to join a video call from the scammer, who claimed to be the CFO of the London head office


利用深偽技術進行的網上投資騙案
EVERYONE CAN BECOME A PARTNER! THE LAW WAS SIGNED
EVERYONE CAN BECOME A PARTNER! THE LAW WAS SIGNED
假
START INVESTING WITH JUST HK$2000 AND WITHDRAW HK$60000 EVERY WEEK!
START INVESTING WITH JUST HK$2000 AND WITHDRAW HK$60000 EVERY WEEK!

90% of all Cyber Attacks Begin with a Phishing Email

Tips to spot Phishing Email 網路釣魚 全攻略

Greed

邊有咁大隻
蛤乸隨街跳

Urgency

十萬火急
幫緊你

Curiosity

開心些牙

Fear

怯 你就輸成世

Practice Makes Perfect!

Mock Phishing Exercise 網路釣魚郵件模擬演習

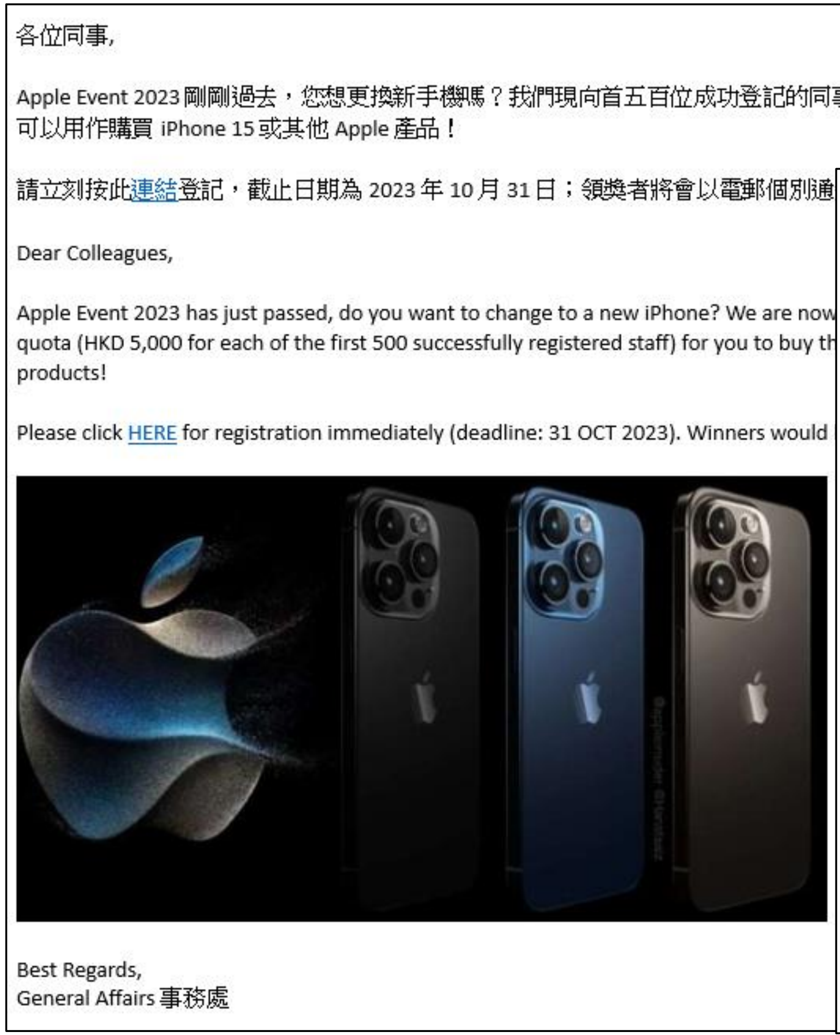
Objective

- Part of overall Cybersecurity Awareness Programme
- Provide a safe and real-life setting for users to experience phishing email
- Create staff awareness on risk of phishing email and best practices

Summary of the Exercise

- Target for staff who have Internet email address
- Leverage a professional phishing campaign platform for the exercise
- Ran for few days for each hospital or healthcare services provider
- Need supports and coordination efforts from management and IT dept

Scenario – “Apple 禮品卡大贈送 Offers for Apple Gift Cards!”



各位同事,

Apple Event 2023 剛剛過去，您想更換新手機嗎？我們現向首五百位成功登記的同事每人送出 HKD 5,000 Apple 禮品卡，可以用作購買 iPhone 15 或其他 Apple 產品！

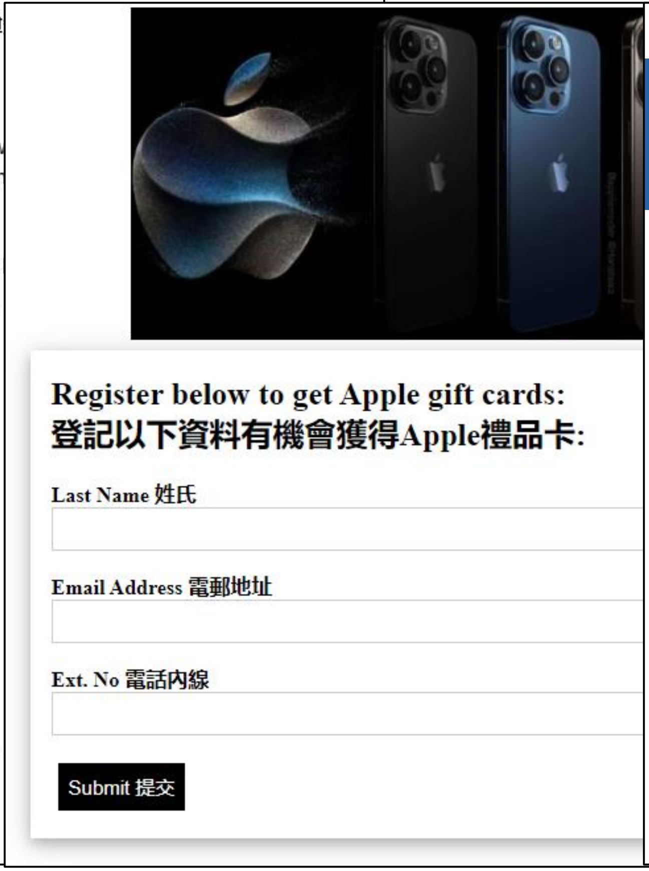
請立刻按此連結登記，截止日期為 2023 年 10 月 31 日；領獎者將會以電郵個別通

Dear Colleagues,

Apple Event 2023 has just passed, do you want to change to a new iPhone? We are now quota (HKD 5,000 for each of the first 500 successfully registered staff) for you to buy th products!

Please click HERE for registration immediately (deadline: 31 OCT 2023). Winners would

Best Regards,
General Affairs 事務處

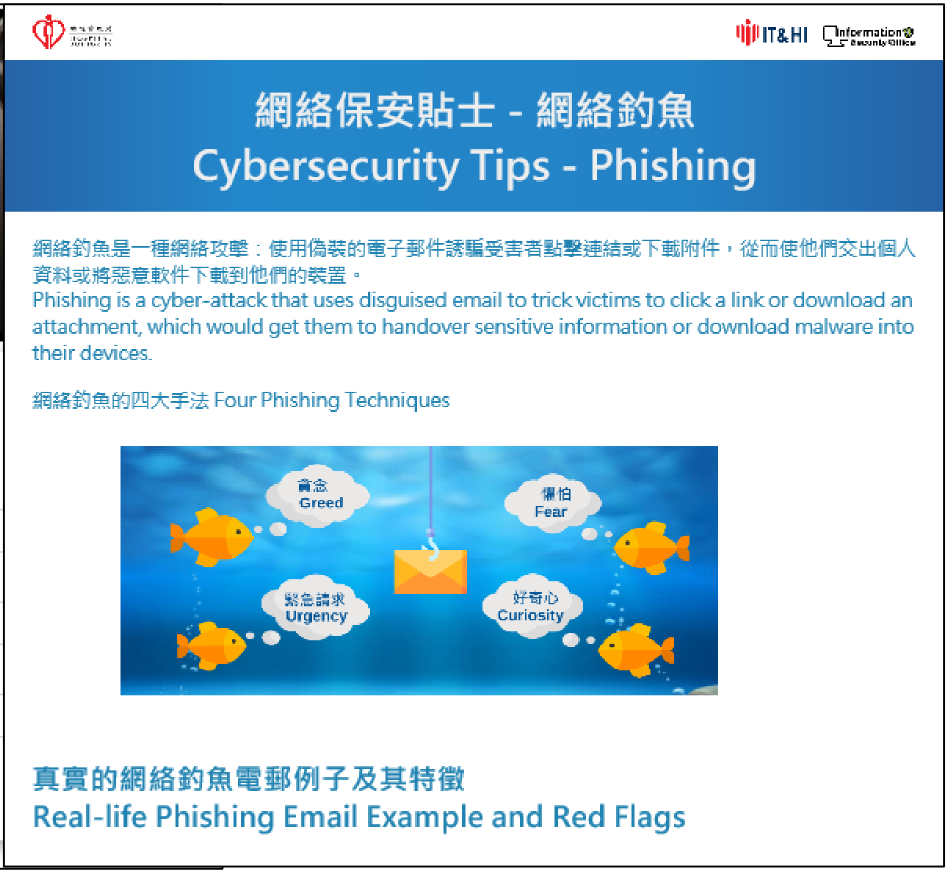


Register below to get Apple gift cards:
登記以下資料有機會獲得Apple禮品卡:

Last Name 姓氏

Email Address 電郵地址

Ext. No 電話內線



網絡保安貼士 - 網絡釣魚
Cybersecurity Tips - Phishing

網絡釣魚是一種網絡攻擊：使用偽裝的電子郵件誘騙受害者點擊連結或下載附件，從而使他們交出個人資料或將惡意軟件下載到他們的裝置。
Phishing is a cyber-attack that uses disguised email to trick victims to click a link or download an attachment, which would get them to handover sensitive information or download malware into their devices.

網絡釣魚的四大手法 Four Phishing Techniques

真實的網絡釣魚電郵例子及其特徵
Real-life Phishing Email Example and Red Flags

Collaboration with Your Trusted Partners

Health Bureau
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

Digital Policy Office
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

醫院管理局
HOSPITAL
AUTHORITY

醫健通
eHealth

香港警務處
網絡安全及科技罪案調查科
Hong Kong Police Force
Cyber Security and Technology Crime Bureau

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Thank you!