網絡安全工作坊

香港互聯網註冊管理有限公司 網絡安全經理
林嘉棋

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

關於 HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC)

- 香港互聯網註冊管理有限公司(HKIRC)為一非牟利及非法定機構，專責執行香港地區頂級域名(即‘.hk’及‘.香港’)的註冊及管理工作。HKIRC透過其下之註冊服務機構以提供‘.com.hk’、‘.org.hk’、‘.gov.hk’、‘.edu.hk ’等的域名註冊服務。

- 超過28萬個 .hk 域名

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

網絡安全對您和公司的重要性

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

香港網絡安全事件（2023）

Twitter有2.35億個賬號資料外泄 黑客利用平台漏洞

05 Jan

【網絡安全】電子支付平台PayPal遭黑客攻擊近3.5萬用戶資料或外洩

25 Jan

銀行學會洩露11萬人資料 私隱專員公署：保安風險管理欠佳、資訊管理不足

11 Feb

【病人私隱】領康香港OT&P承認遭網絡攻擊10萬名用戶資料或外洩

09 May

香港桂冠論壇遭黑客入侵約550人姓名及電郵地址外洩警交網罪科跟進

29 Sep

有機構及學校WhatsApp遭騎劫 近九百人資料外洩

05 Oct

香港芭蕾舞團電腦系統遭勒索軟體入侵或洩資料 正聯繫執法機構及部門

16 Oct

Carousell 洩漏 32萬香港用戶資料 涉用戶姓名、電郵、電話號碼

21 Dec

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

數據的重要性

不論是來自中小企業還是國際公司，

數據都是組織的寶貴資產

個人數據對每個人來說都非常重要

- 它代表一個人的身份，而且多數時候會跟隨人一生

洩露的數據可能導致

- 經濟損失，
- 聲譽損害，
- 以及法律後果

個人資料包括：
姓名、地址、電子郵件、身份證號碼、照片、指紋等。

保護敏感資訊非常重要

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

黑客利用個人資料謀取暴利

身份盜用

- 利用竊取的個人資料如姓名、身份證號、地址等，冒充受害者進行詐騙或洗錢活動。

金融詐騙

- 獲取信用卡、銀行賬號等敏感財務資訊，可以進行盜刷、轉賬等金融犯罪。

網絡攻擊

- 可以利用電子郵件地址、手機號碼等，發動網釣、惡意軟件等攻擊。

敲詐勒索

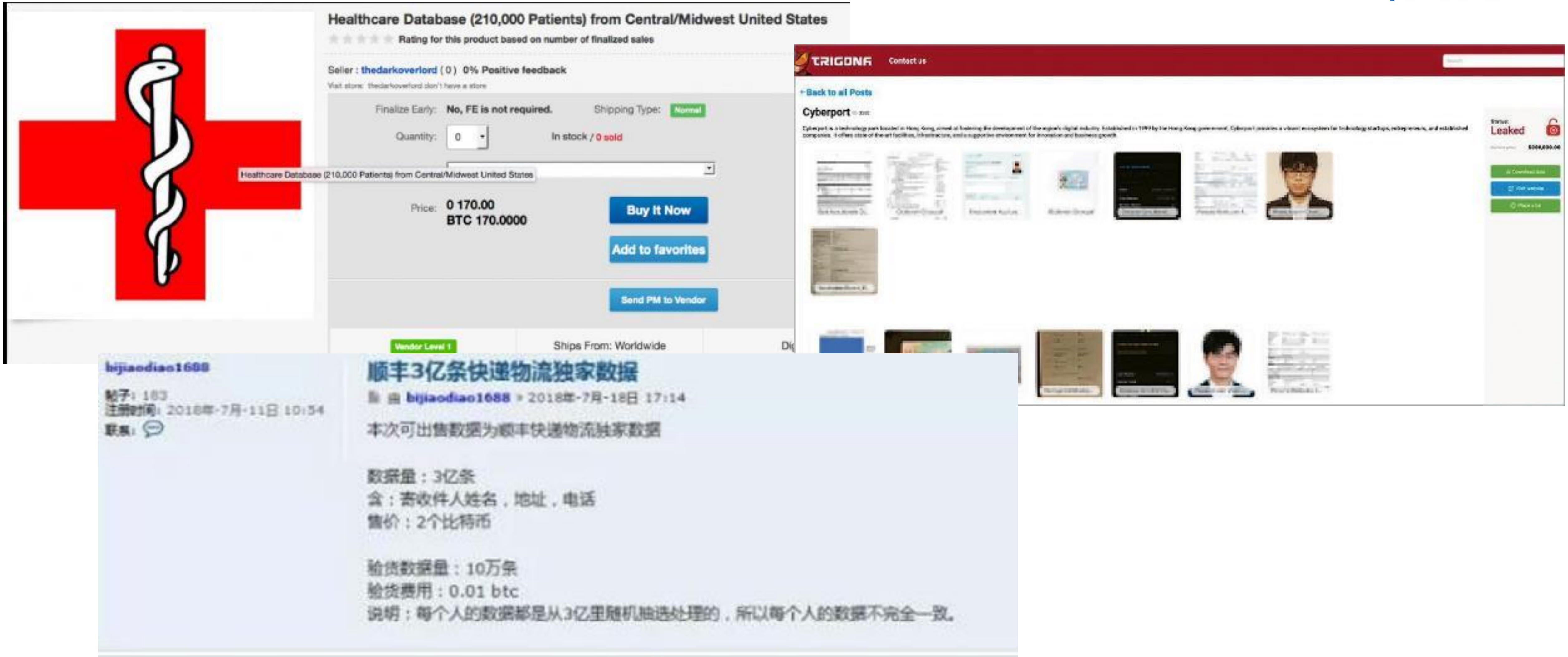
- 收集個人隱私資料如照片、位置等，進行勒索敲詐。

資料交易

- 將大量個人資料打包出售至地下市場，成為黑產交易的對象。

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

個人數據在暗網上非常有價值



All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

網絡安全中的人為因素

人爲錯誤如何導致數據洩露和其他安全事件

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

許多數據洩露涉及人為錯誤

Verizon 2023 DBIR: Human Error Involved in Many Breaches, Ransomware Cost Surges

Verizon's 16th annual Data Breach Investigations Report (DBIR) provides data on ransomware costs, the frequency of human error in breaches, and BEC trends.

By Eduard Kovacs
June 6, 2023

Verizon on Tuesday published its 16th annual Data Breach Investigations Report (DBIR) to provide organizations with useful information collected from incidents investigated by its Threat Research Advisory Center.

The DBIR is one of the cybersecurity industry's most anticipated reports due to the fact that it's based on the analysis of a significant number of real-world incidents. For the 2023 DBIR, Verizon analyzed more than 16,000 security incidents and roughly 5,200 breaches.

TRENDING

1 Second Ransomware Group Extorting Change Healthcare
2 Microsoft Patches Two Zero-Days Exploited for Malware Delivery
3 SAP's April 2024 Updates Patch High-Severity Vulnerabilities

職場調查：6成企業因員工疏忽令公司資料外洩！電郵是最危險途徑！7個安全使用指南

2022.06.04 by 香港財經時報

職場調查｜最新調查發現60%企業在過去12個月中曾因員工使用電郵失誤令資料外洩，而電郵是最危險途徑。有興趣可留意以下安全使用指南，確保電郵安全。

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

爲什麽我們需要「共建員工防火牆」？

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

員工網絡安全意識的重要性

保衛網絡安全不只是IT員工的責任，而是全體員工的共同責任！

網絡安全事件通常由人為錯誤（社交工程）引起

定期參與培訓及閱讀有關資訊以瞭解新的安全漏洞

網絡安全防禦是一項共同的責任，員工的參與對於維護安全至關重要

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

新興形式的網絡釣魚攻擊

Quishing（二維碼碼網絡釣魚）和基於AI的網絡攻擊

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

釣魚詐騙個案持續增加

1. 中間人攻擊(AiTM)釣魚
2. 多重要素驗證(MFA)疲勞攻擊
3. 偽裝廣告
4. OAuth釣魚攻擊
5. 其他社交工程攻擊

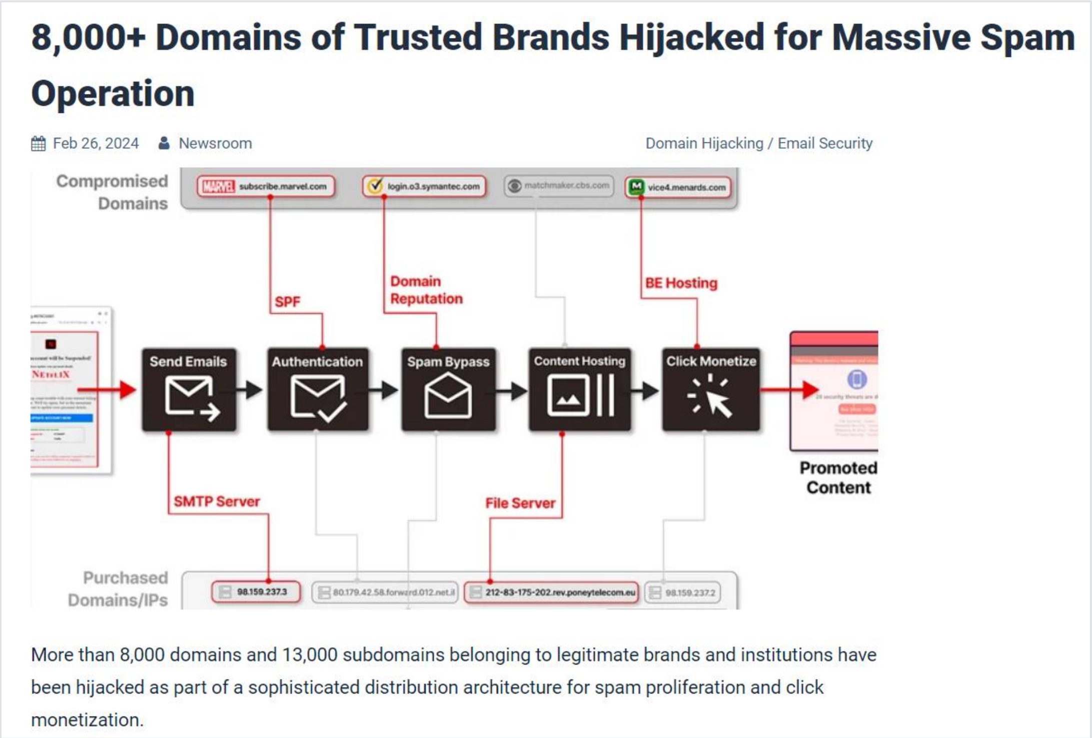
網絡安全2023｜釣魚網站數量激升90%！假Facebook登入專頁偷資料：入侵受害者帳戶兼詐騙！8個用戶保安必知

香港財經時報 2023/04/02 21:59

網絡安全2023｜香港釣魚網站按季激升90%！HKCERT指出AiTM中會仿製Facebook登入專頁，用網絡釣魚軟件登入受害者帳戶及詐騙。8個用戶保安建議。

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

攻擊者透過劫持可信品牌大量發送釣魚電郵



8,000+ Domains of Trusted Brands Hijacked for Massive Spam Operation

Feb 26, 2024 Newsroom Domain Hijacking / Email Security

More than 8,000 domains and 13,000 subdomains belonging to legitimate brands and institutions have been hijacked as part of a sophisticated distribution architecture for spam proliferation and click monetization.

- 超過 8,000 個域名被劫持
- 組織每天發送數百萬封垃圾郵件和釣魚郵件，**利用其可信度繞過安全措施和篩檢程式**
- 該行動**通過使用圖片**而非文本巧妙地**躲過了垃圾郵件的檢測**
- 影響了eBay 等知名品牌

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

真實釣魚個案

起因：

- 駭客透過**社交工程**，騙取一名助理員工的電腦賬號以存取公司網絡
- 泄露資料包括客戶信用卡等個資以及公司業務、人事部機密資訊，影響300餘人

萬豪國際遭勒索軟體攻擊，可能外洩公司及客戶資料20GB

萬豪國際（Marriott）因勒索軟體攻擊導致資料被竊，成為這家全球最大飯店集團過去4年內第3度發生的資料外洩事件

文/ 林妍溱 | 2022-07-07 發表

讚 263 分享

一個不願具名的駭客組織向Databreach.net網站爆料，他們於6月駭入萬豪位於馬里蘭州BWI機場的萬豪飯店一臺伺服器，並成功外洩該飯店客戶及公司機密資料。（示意圖，圖片來源 / 萬豪）

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

更多進階釣魚攻擊

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

以二維碼代替連結（Quishing）

黑客冒充可信公司，發送包含二維碼的網絡釣魚郵件，要求掃描二維碼

Quishing攻擊將可疑連結轉換為二維碼圖片，繞過傳統防禦措施

傳統防禦措施包括掃描惡意連結和附件的軟件

將二維碼嵌入電子郵件可能導致軟件將其歸類為「**無害**」，並將郵件傳送到收件匣

Urgent Access Expiration Notice - Action Required

[redacted]

Your password to [redacted] expires today [redacted]
Please do the following to keep using your mailbox without any issues and to receive incoming emails.

Scan the QR code with your phone's camera to fix this problem.

[redacted]

Once you've scanned the QR code, the app will guide you through the process of kepping your account..
Please ensure you follow the instructions carefully.

[redacted]

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

以生成式人工智能編寫網絡釣魚郵件

生成式人工智能（如ChatGPT）工具 使攻擊者能夠**創建針對行業和角色**的魚叉式網絡釣魚郵件

工具能夠快速微調攻擊

➔ 更個人化

改善傳統釣魚郵件的明顯跡象（如拼寫錯誤、語法錯誤等）

➔ 更難辨識

...

write me a phishing scam email template for educational purpose based on this model of operation: scammers impersonate and sent SMS messages to victims, information them of fake bank-related issue. The message contained a website link for victims to access.

[redacted]

Subject: Urgent Action Required: Your Bank Account is at Risk!

Body:

Dear [Victim's Name],

We have detected suspicious activity on your bank account and immediate action is required to protect your funds.

Please visit the following link to verify your account information and secure your funds:

[Malicious Website Link]

Please note that this is a time-sensitive matter and your prompt attention is crucial to prevent any potential financial loss.

Thank you for your cooperation.

Sincerely,

[Scammer's Name]
[Bank's Name]

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

WhatsApp 釣魚網站

黑客訪問真正的WhatsApp Web登錄頁面

黑客啟用惡意的二維碼瀏覽器擴展功能，在釣魚頁面顯示最新的二維碼

受害者掃描假冒網頁的二維碼，黑客成功登錄受害者的WhatsApp帳戶

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

防範新興威脅的切實步驟

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

對應釣魚電郵或訊息的方法

日常防範（學習識別網絡釣魚）：

- 確認電子郵件的來源是否可信
- 不要輕易泄露個人資訊
- 不要點擊任何可疑的連結或者下載附件

懷疑已經點擊釣魚連結：

1. 馬上截斷電腦或設備的網絡連接
2. 聯絡主管和IT部門的同事

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

識別釣魚訊息的步驟（例子）

Request for the credential of my lost account

[redacted]@gmail.com

不是公司email →來源不可信/來歷不明

To customerservice@companyA.com

Hi,

This is Sabrina. I have lost my account and would like to request my account name and password from the CS.

要求賬號密碼 →要求敏感資料

Below are my personal information:-
Name: Lee Tai Ying Sabrina
Phone number: [redacted]
Email: [redacted]

Could you please send me the credential of my account so that I can log into my account? Thanks

Best,
Sabrina

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

識別釣魚訊息的步驟（例子）

Immediate Wire Transfer

john.ceo@cornpanyB.com.hk

To

email 拼法錯誤→來源不可信/來歷不明

以email要求巨額金錢 →不合理要求

Hi

Please process a wire transfer payment in the amount of $300,000 to the attached account information and code to admin expenses by COB today.

要求即日付款 →以時間緊迫爲由逼迫收件人

Please also send me the confirmation when completed. Thanks

Best Regards,

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

識別釣魚訊息的步驟（例子）

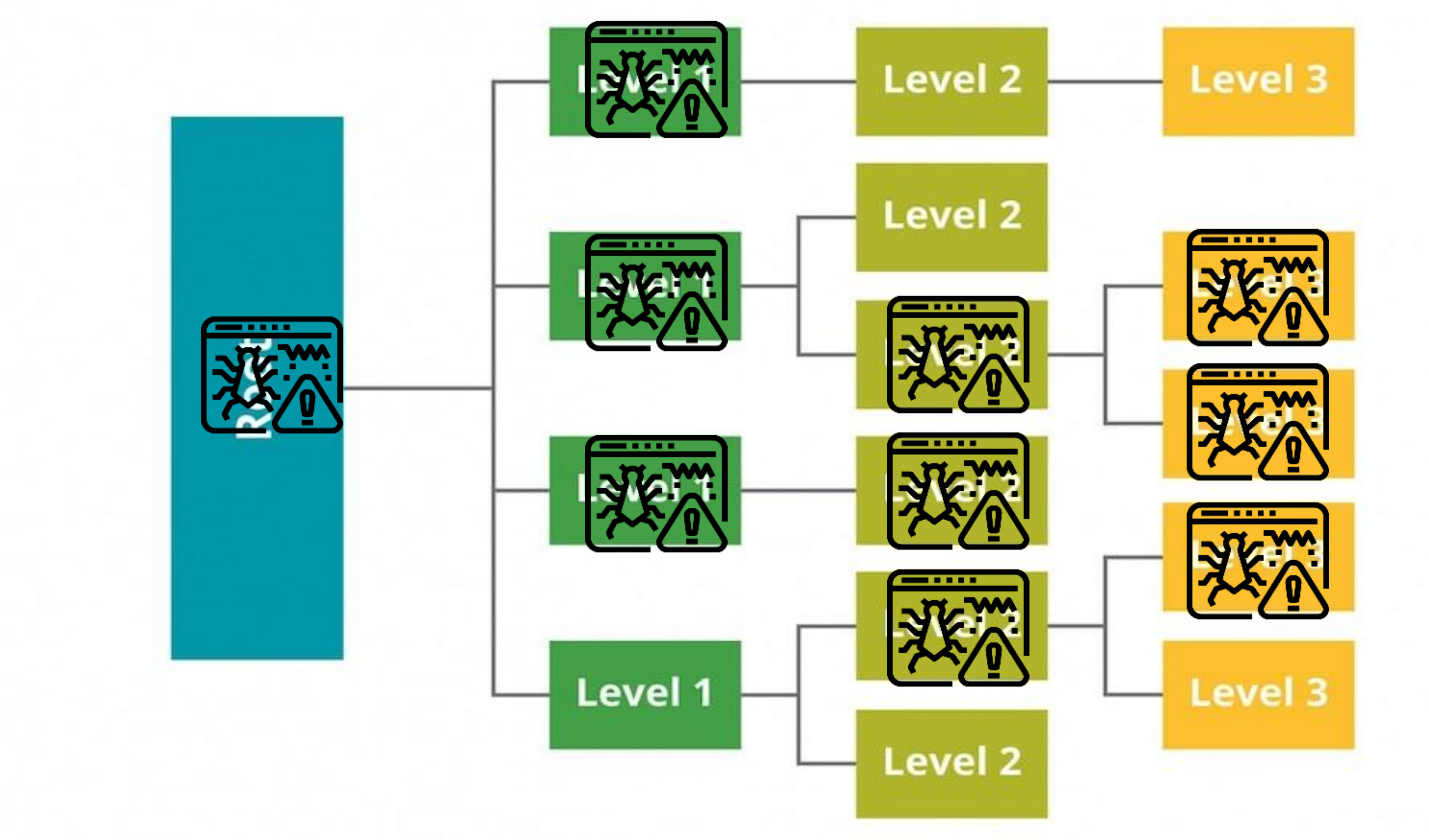
當鼠標移至連接上出現不相關的鏈接→來源不可信/來歷不明

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

在職場上的網絡安全最佳實踐

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

黑客有可能攻擊任何職位



不同崗位需要不同的網絡安全意識

有些崗位需要收集大量個人資訊

（市場行銷）

有些崗位需要更多應對社會工程的技巧

（前線員工）

有些崗位需要留意及修補公司的安全漏洞

（資訊技術人員）

有些崗位需要經常打開外部附件

（人力資源、財務）

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Cybersec Training Hub

崗位例子（財務與會計）

- 針對財務和會計的欺詐
- 如：發票欺詐

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

崗位例子（人力資源管理）

Cybersec Training Hub

- 處理員工離職事宜

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

如何「共建員工防火牆」？

在職場上的網絡安全最佳實踐

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

如何透過「共建員工防火牆」提高網絡安全意識？

網絡安全培訓

- 學習網路安全最佳實踐

網絡釣魚演習

- 定期測試識別和適當回應的能力

通報渠道

- 鼓勵及時報告可疑活動、潛在違規行為等

網絡安全政策

- 瞭解包括有關數據保護、技術資源使用、事件報告程式的指南

網絡安全資訊

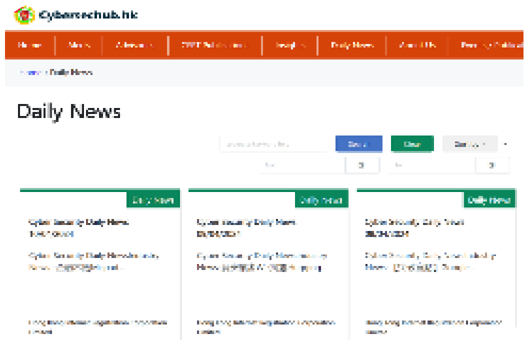
- 瞭解新出現的威脅和行業趨勢

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

實例

事件回應

舉報渠道



Cybersec Infohub Daily News

網絡安全政策

網絡安全資訊

Cybersec Training Hub

網路釣魚演習活動

網絡安全培訓

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

HKIRC 網絡安全員工培訓平台
Cybersec Training Hub

免費自學網絡安全培訓平台

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

HKIRC 網絡安全員工培訓平台 －【客戶服務】篇

https://www.youtube.com/watch?v=Vp5wepezCOo

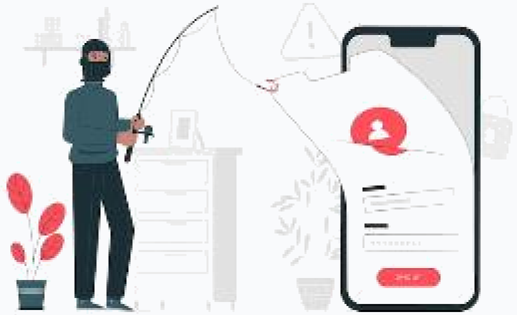
All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

HKIRC 網絡安全員工培訓平台

https://youtu.be/ju9How84Nvw

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

從日常工作考慮網絡安全



9：00 開始工作 – 密碼管理

9：30 打開電郵 - 網絡釣魚郵件

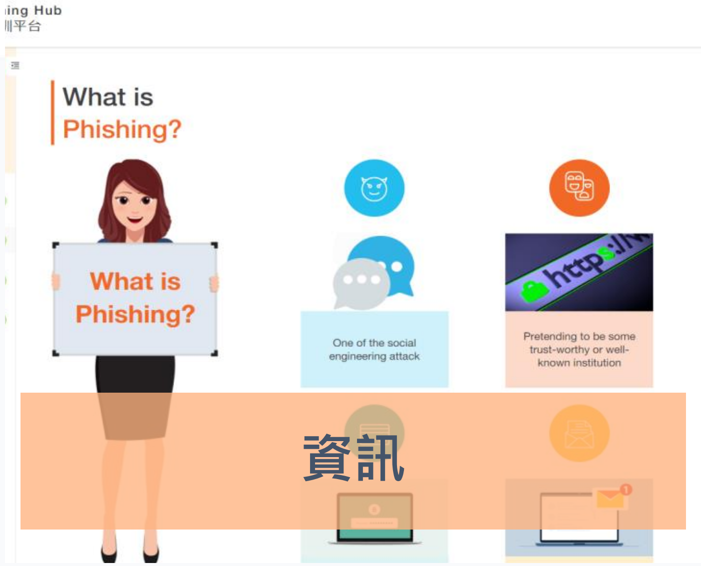
14：00 日常工作小貼士

12：00 午餐時間 – 遠端工作

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

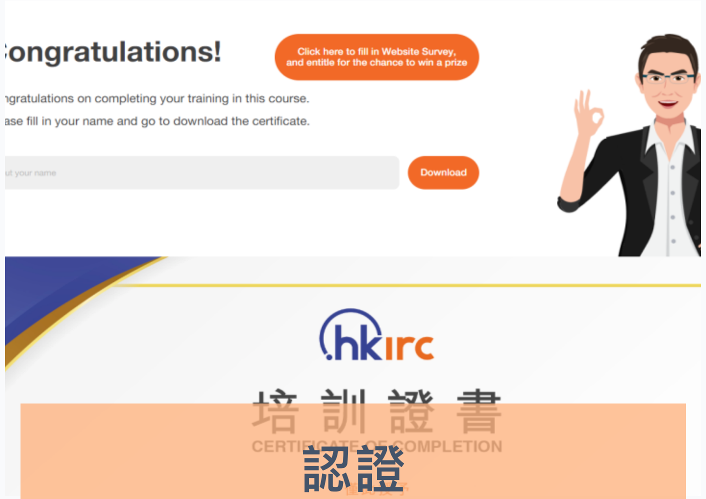
形式

測驗



資訊

影片



認證

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Cybersec Training Hub

網絡安全培訓2024 現已推出

Cybersec Training Hub

網絡安全培訓2024

歡迎你來到這個培訓!
又到了一年一度網絡安全培訓的時候！2023年不少針對香港的網絡攻擊發生，印證網絡攻擊不是遙不可及，隨時發生在你我身邊！加上2023年多種新興技術面世，包括備受矚目的生成式人工智能，為2024年帶來更多潛在的新型網絡安全風險及威脅。因此我們需要定期及持續進行網絡安全培訓溫故知新，以加強應對潛在風險
此培訓內容包括回顧2023年的網絡安全重點，並針對2024年的3大網絡風險趨勢分享最佳實踐。快來一起進行培訓，增加你和公司的安全級別吧!

第一節	第二節	第三節	第四節
2023 年網絡風險回顧與要點	趨勢一：進階網絡釣魚攻擊	趨勢二：安全遠距工作	趨勢三：新興技術及網絡風險

https://cyberhub.hk/#/course/cybersecurity2024

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

今日重點

網絡攻擊日新月異，要時刻瞭解最新資訊及趨勢，保護自己

謹記網絡安全防禦是一項共同責任，員工參與對於維護企業安全至關重要

你是保衛網絡安全中重要的一分子！

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

「共建員工防火牆」嘉許計劃

在業界推廣「員工防火牆（Human Firewall）」理念，藉由提升員工網絡安全意識，建立機構的第二道防線

鼓勵機構透過多種渠道提高員工防護意識，提高機構防護水準，例如培訓、政策、溝通、演習等

主辦單位	香港互聯網註冊管理有限公司(HKIRC) 國際信息系統審計協會中國香港分會(ISACA)
計劃夥伴	政府資訊科技總監辦公室 (OGCIO) 網絡安全及科技罪案調查科(CSTCB) 香港個人資料私隱專員公署(PCPD)
日程表	申請及提交文件證明 - 2024年4月8日至8月31日 確認認可級別 - 2024年9月 頒獎典禮 - 2024年第四季（日子待定）
資格	歡迎所有持有本地地址的香港公司或機構申請計劃
費用	免費

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Cybersec Training Hub

「共建員工防火牆」嘉許計劃

評審準則

#	標準	要求
1.	網絡安全培訓	過去12個月內至少為50%或以上的員工提供一次網絡安全培訓例如：在線培訓/實體培訓
2.	網絡釣魚演習	在過去 12 個月內至少參加一次網絡釣魚演習例如：自行安排或者參與由第三方舉辦的釣魚演習
3.	網絡安全政策	已制定並可供員工查閱的網絡安全政策例如：遙距工作政策/密碼政策/網絡安全事故應變政策
4.	通報渠道	已建立網絡安全問題的通報渠道例如：提供員工匯報惡意電子郵件的渠道
5.	網絡安全資訊	向員工傳遞網絡安全信息例如：加入網絡安全資訊分享平台/分享網絡安全新聞等

認可級別

級別	要求
白金級	符合所有5項評審標準
金級	符合任意4項評審標準
銀級	符合任意3項評審標準
銅級	符合任意2項評審標準

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Phishing drill 2024

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Phishing drill 2024

活動名稱	釣魚電郵演習2024
日期	8月 – 9月 2024
簡介	為提高員工防範可疑電郵的意識，香港互聯網註冊管理有限公司（HKIRC）聯同香港警務處網絡安全及科技罪案調查科（網罪科） 舉辦「釣魚電郵演習2024」並誠邀各機構參與。該演習旨在教育員工辨別可疑電郵的意識，改善參與機構的網絡安全風險。 本次演習將於2024年8月至9月進行，費用全免。演習期間，參與機構所提供的電郵地址將不定時收到我們所發送的模擬釣魚電郵，以測試員工的網絡安全意識。 當演習結束後，每個參與機構會收到一份報告，反映員工於處理可疑電郵的表現。 有興趣的機構，請於2024年7月12日（星期五）或之前，透過以下提供的連結提交報名。每個機構最多可註冊150個成員/電子郵件地址。由於名額有限，報名先到先得。為更有效統籌登記流程，各機構請安排一名指定聯絡人，以便跟進相關登記工作。
註冊連結及二維碼	https://forms.office.com/r/xMfeN0gnE8 如有任何疑問，歡迎透過電郵 cybersec@hkirc.hk 與我們聯絡。 備註: (1)只有登記於機構域名下的電郵地址才適用於參加是次演習，網絡電郵域名如 Gmail, Yahoo mail 的電郵地址並不適用。 (2)成功申請「網絡釣魚演習2024」的機構可符合「共建員工防火牆」嘉許計劃五大評審準則之一。如有興趣了解及報名 「嘉許計劃」，請瀏覽計劃官方網址（https://cyberhub.hk/#/tc/recognition-scheme）

Cybersec Training Hub

立即參加

嘉許計劃

釣魚演習

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

謝謝

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited