

# 網絡安全員工培訓平台

香港互聯網註冊管理有限公司 網絡安全經理  
林嘉棋

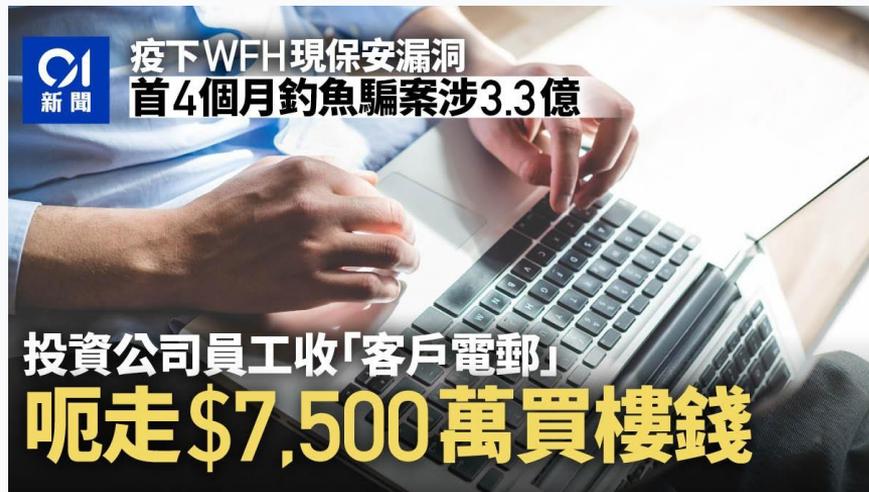
# 不顧網絡安全的後果

- 洩漏敏感數據
- 失去捐款人和支持者的信任
- 長遠影響組織聲譽
- 罰款、額外審查和其他損失



## 真實本地個案

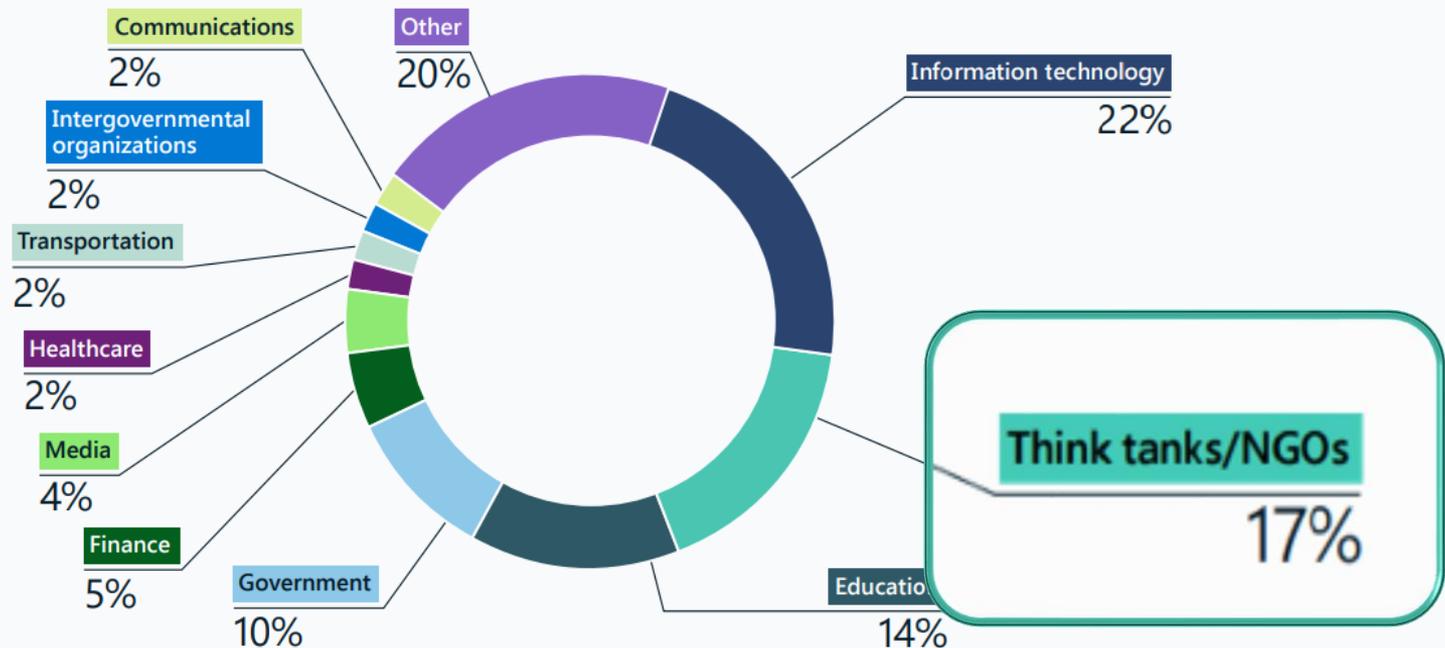
- 美資投資公司員工
- 聲稱是公司客戶的釣魚電郵
- 匯入960萬美元（拆合約7,500萬港元）到騙徒戶口



# 微軟 2022 年數位防禦報告

最常被網絡攻擊的行業分類

Industry sectors targeted by nation state actors



# 為甚麼罪犯會攻擊NGO？

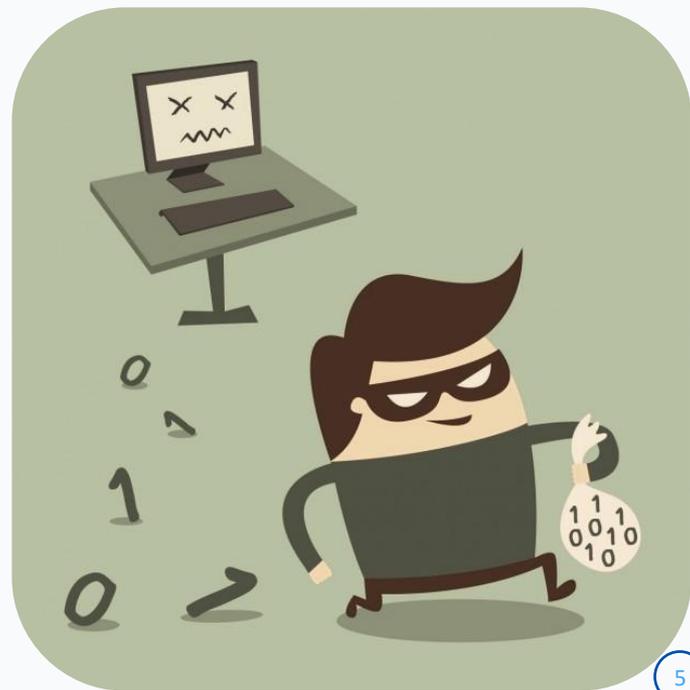
- 持有捐款者、受益人等的資料、數據 

→ 竊取資料、妨礙NGO活動

- 網絡保安方面  預算較低

→ 缺乏安全意識

缺乏嚴格的保安措施 = 容易攻擊 



# 數據泄漏的主要原因

- 過時、甚少進行更新的安全軟體
- 惡意軟體
- 物理盜竊 ...

- 人為錯誤
- 社會工程

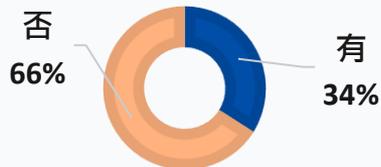


# 網絡安全員工培訓平台 (Cybersec Training Hub) 平台簡介

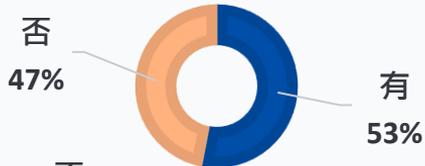
# 香港員工網路安全培訓調查

擁有IT部門/全職IT人員

公司規模：1-10  
微型企業



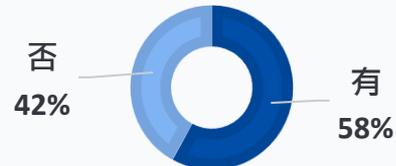
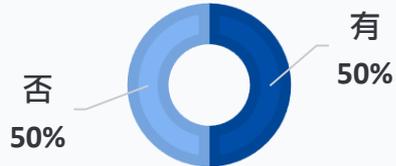
公司規模：11-50  
中型企業



公司規模：>50  
大型企業



雇主安排  
入職時進行網路安全培訓



約24萬間公司、140萬勞動力缺乏網路安全培訓

# 網絡安全意識



## 現狀



## 處於危險之中⊗

- 根據過往經驗工作
- 不小心提防風險

## 有平台幫助

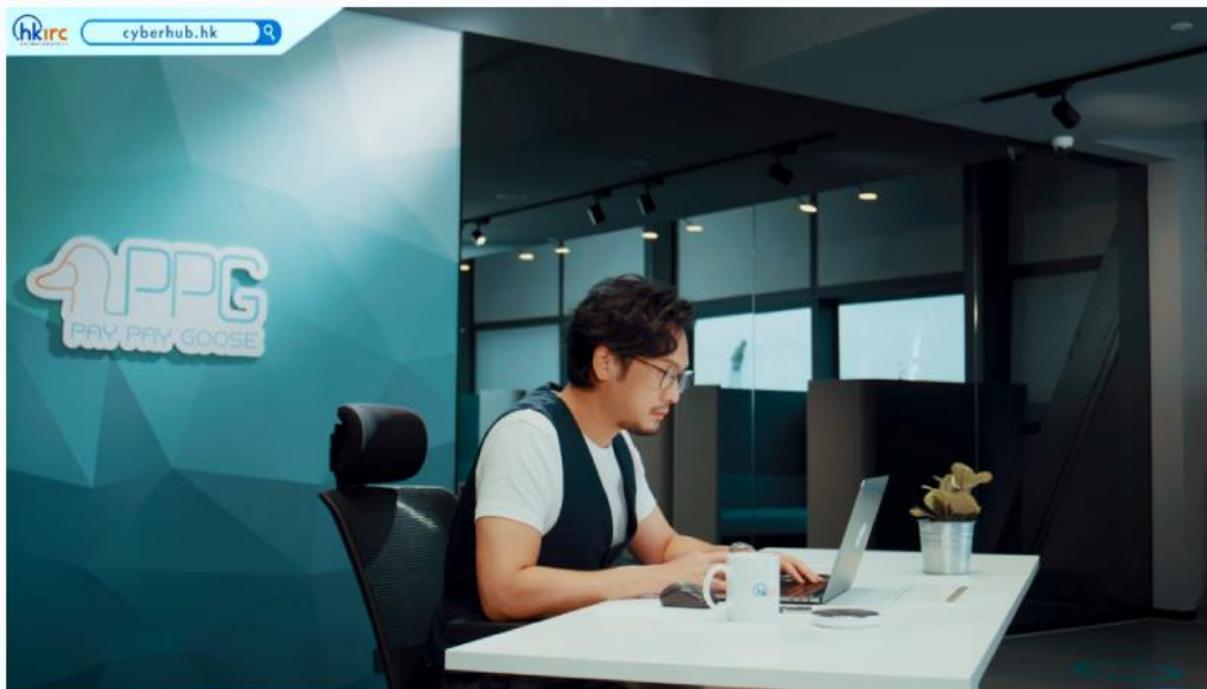


## 更安全☺

- 了解行業標準（例如遠端工作）
- 了解及注意潛在風險

# Cybersec Training Hub

<https://youtu.be/ju9How84Nvw>



# 主要特點



完全免費的在線自  
學專業培訓



無需技術背景適合  
所有員工



貼近現實工作環境  
的培訓內容



培訓後頒發電子證  
書方便公司管理

# 形式



## Quiz

Select the correct answer

Tom received a phishing email containing a link that he accidentally clicked, but nothing happened. Then he was notified by the antivirus software that an unknown virus had been detected, which he thought it was because of the phishing email.

What should he do next is the most important?

- A. Do nothing
- B. Disconnect the computer or device from the internet or network
- C. Tell supervisor
- D. Inform the IT staff at the company

## 測驗

## 9:30 am Open Email

The first thing to do is to check your mailbox after successfully logged in!  
Will you open all the email and click the link or attachment inside?

Transcript 字幕

## 影片

## What is Phishing?

One of the social engineering attacks

Pretending to be some trust-worthy or well-known institution

資訊

## Congratulations!

Click here to fill in Website Survey, and enter for the chance to win a prize.

Congratulations on completing your training in this course.  
Please fill in your name and go to download the certificate.

[Download](#)

## 培訓證書 認證

CERTIFICATE OF COMPLETION

# 適合不同目標群體



第1階段

一般員工



第 2 階段

工作性質

如：

- 高級管理層
- 財務與會計
- 人力資源



第3階段

特定行業

如：

- **NGO**
- 零售
- ...

# 基本員工培訓 – 從日常工作角度設計



9 : 00 開始工作 – 密碼管理



9 : 30 打開電郵 - 網路釣魚郵件

14 : 00 日常工作小貼士



12 : 00 午餐時間 – 遠端工作



# 工作性質例子 (高級管理層)

- 保護公司

## 損害 公司品牌形象

### 域名搶註

搶先一步登記公司的網路域名後，再高價賣給該公司



香港曾經有一名學生，搶註了和記黃埔的中文域名後，在他的個人網站上開價100萬美金出售這個域名。

### 社交媒體冒充

偽造社交媒體帳戶去冒充真實的帳戶以欺騙用戶



網絡犯罪分子冒充社交媒體LinkedIn向用戶發送釣魚電郵，欺騙受害者至虛假的登錄頁面登入。

### 電子郵件欺騙

使用偽造的發件人地址發送電子郵件，如：假冒企業高層



有騙徒入侵跨國公司行政總裁的帳戶，以事態緊急為由要求員工將款項匯至指定銀行帳戶，涉及金額達2.7億港元。

### 假冒網站

偽造相似網站以誤導讀者其為官方網站



[查看示例](#)

有騙徒偽冒港鐵的網站邀請市民參與顧客滿意度調查，以獲取五張免費單程車票的獎賞。

# 工作性質（財務與會計）

- 針對財務和會計的欺詐
- 如：發票欺詐

## 發票詐騙（冒充供應商）

### 發票詐騙



什麼是發票詐騙？



01

是社交工程攻擊的其中一種形式



02

透過冒充公司的供應商、商業夥伴或公司高層



03

以欺騙公司員工匯款至騙徒戶口

## 如何防止商業電郵騙案

### 如何防止商業電郵騙案

於 2020 年，香港警務處接獲 639 宗商業電郵騙案，合共損失超過 22 億元，即平均每宗案件損失近 350 萬元，當中有七成的受害人公司為本地的中小企業。

我們一定要保持警覺，才不會輕易墮入詐騙陷阱！



01

不要輕信突然改變的匯款要求

# 工作性質（人力資源管理）

- 處理員工離職事宜

## 公司賬號的存取權限

離職員工  
存取權限的安全處理



## 公司資產的安全

公司資產的安全

一定要確保員工在離職前把這些公司資產歸還!



## 針對NGO業界的培訓內容（預備中）

以「利用第三方工具的注意點」為例：

- 第三方工具（例如Free PDF Converter）的使用風險
- 找到安全的第三方工具的方法



# Being Alerted after Training!



<https://www.youtube.com/watch?v=GCiDVoBWx7o>



Cybersec Training Hub  
網絡安全員工培訓平台

免費 | 專業 | 一站式平台

員工網絡安全培訓  
必睇網站



cyberhub.hk



# 共用資訊 了解網路安全趨勢



# 網絡安全資訊共享夥伴計劃 (Cybersec Infohub)

- 共同管理計劃：
  - 政府資訊科技總監辦公室 (OGCIO) 及
  - 香港互聯網註冊管理有限公司(HKIRC)
- 促進本地不同界別的網絡安全持份者之間緊密的合作
- 會員可以在平台上共用網路安全資訊，攜手防禦網路攻擊



主要互聯網  
服務提供者



關鍵基礎設施營運商



金融與保險



創新與技術與資訊安全



教育

GovCERT.HK



香港電腦保安事故  
協調中心



其他行業



## 會員制度

- 任何營業位址位於香港並擁有香港地區頂級域名(即'.hk'及'.香港')之本地機構
- 管理電子通信網路和對網路安全資訊有運營需求
- **免費**申請





## 計劃優點

參與計劃可享多項優勢，包括：

參加會員專享活動（如：研討會、技術工作坊、業界會議等）

與不同界別的成員建立互信關係及聯繫

接收來自不同界別專家的網絡威脅預警資訊和心得

有機會與網絡安全專家協作和聯繫

可選擇匿名發表！



# 計劃亮點

- ✓ 面向 IT 專家和企業用家的網路安全資訊
- ✓ 最新功能/服務/活動：

每日快訊



Cybersec Connect



網絡安全星期三



機器對機器威脅情報分享



會員活動



## HKIRC「網健通」服務 (HKIRC「Healthy Web」Services)



HKIRC 一向重視並致力維護「.hk」用戶的網絡安全。為了進一步提高「.hk」用戶網站的安全性，HKIRC 將會於2023年推出全新的網站保安檢測服務—「網健通」，主動協助「.hk」用戶檢視其網站的安全狀況並提供簡要報告。**服務內容包括：發現及提醒網站有任何潛在風險，例如不當的網絡安全設定或使用已過時網站伺服器**等，希望用戶能及早提高警覺，以採取相應行動保護其網站，遠離網絡威脅。

「.org.hk」域名為此計劃的首批特選用戶，將優先享用此服務。HKIRC會在今年三月至四月期間向「.org.hk」用戶發放「網健通」報告，通知檢測結果。假如收到報告後有任何疑問，可以發電郵到 [cybersec@hkirc.hk](mailto:cybersec@hkirc.hk) 查詢，謝謝！

申請連結: <https://forms.office.com/r/TEPh4i67Hz>

1. 為免生疑問，「網健通」透過瀏覽網站的公開資訊，以非侵入形式來評估網站的安全性，並向用戶提供良好作業模式和提高整體網站安全性的實用建議。
2. 若用戶未有收到HKIRC「網健通」的檢測報告，並不等於閣下的網站沒有網絡保安問題。
3. 「網健通」不會測試SQL注入漏洞、CMS插件、不正確的密碼創建策略或存儲過程等。這些與「網健通」測試的內容一樣重要，網站運營商不應僅僅因為他們在網健通得到不錯的結果而忽視它們。
4. 本「網健通」服務受其適用條款和條件嘅約束。HKIRC對服務（包括報告的完整性或準確性）不作任何形式的保證。

HKIRC 免費服務簡介 - 「網健通」



首批特選用戶「.org.hk」域名

立即免費申請

# 感謝