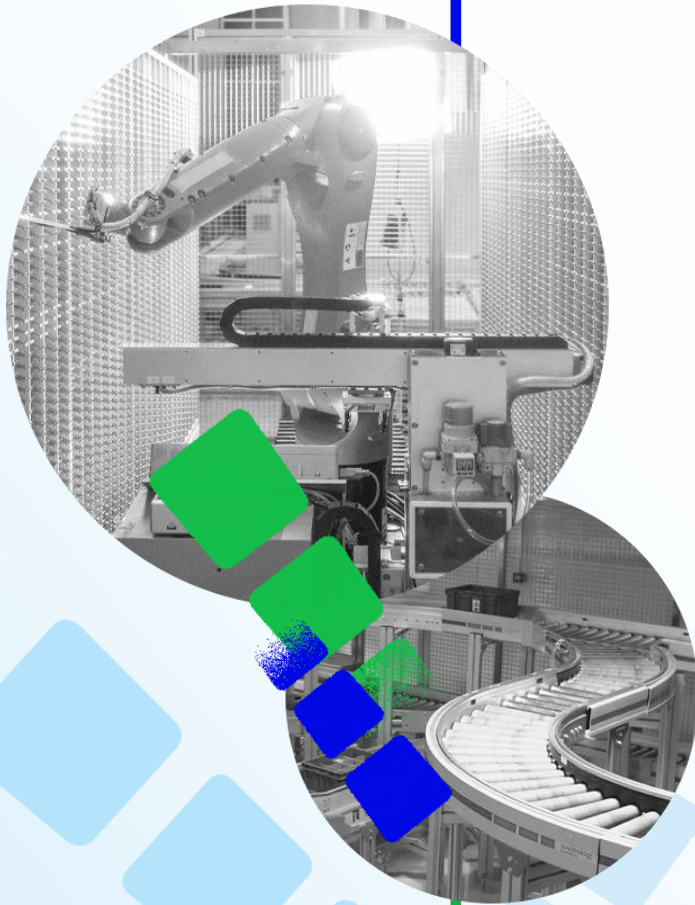


中小企防範網絡攻擊 研討會

陳仲文工程師

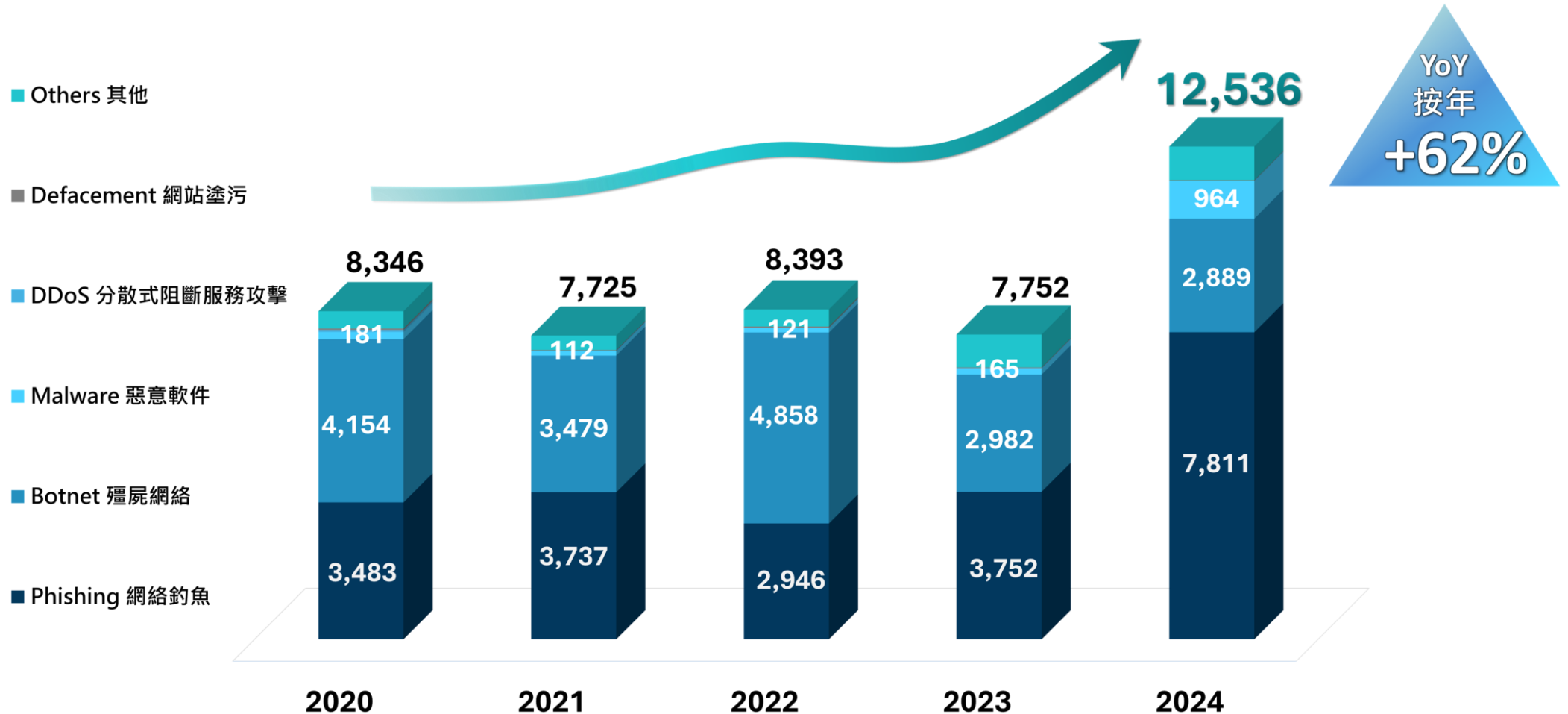
生產力局數碼轉型部總經理
兼HKCERT發言人

2025年3月20日

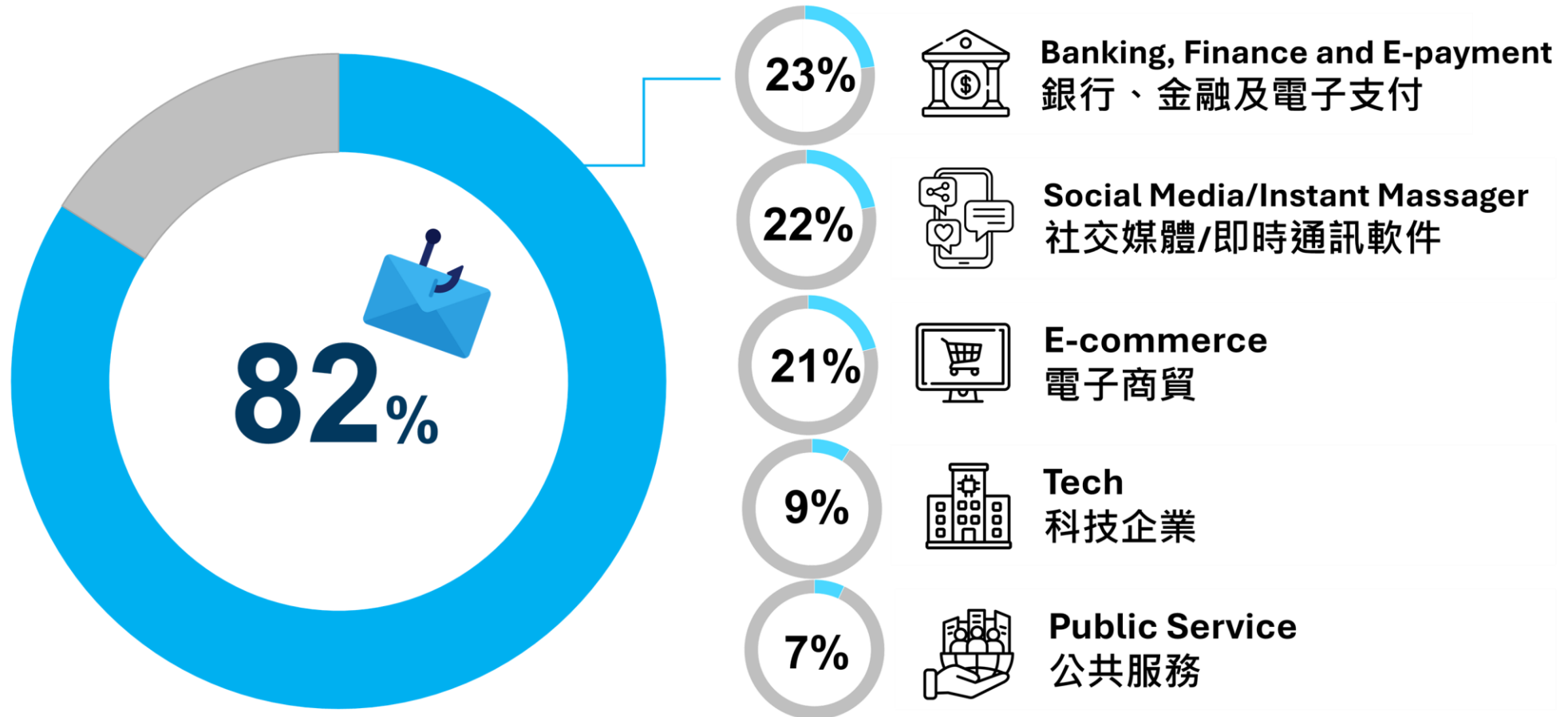


“ 回顧 2024 ”

Trend of Security Incidents (No. of Cases) 保安事故宗數走勢



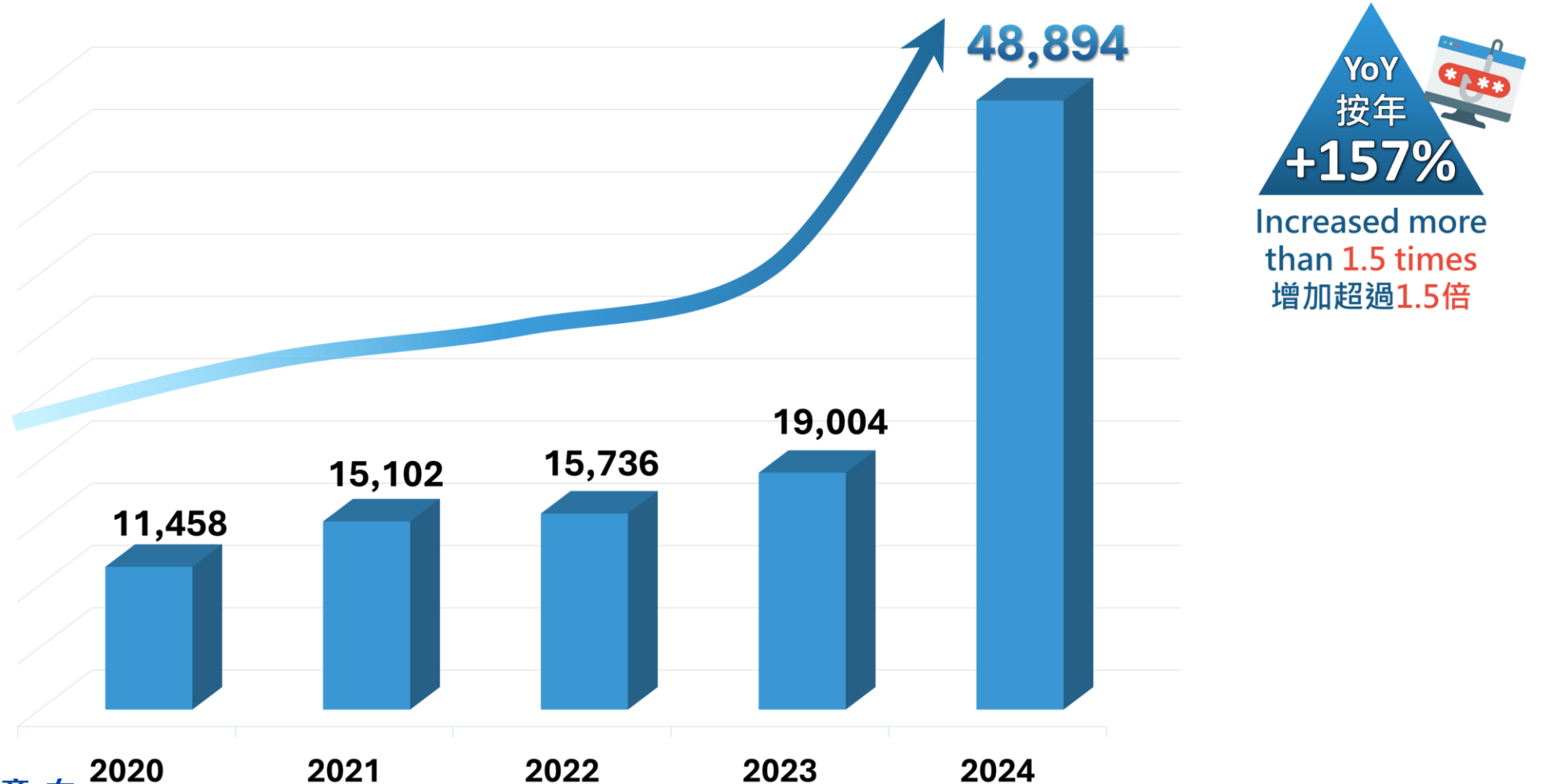
Top Five Industries Targeted by Phishing in 2024 2024年頭五個行業遭受釣魚攻擊分佈統計





Hong Kong Computer
Emergency Response Team
Coordination Centre
香港網絡安全事故協調中心

Trend of Phishing URL 網絡釣魚所涉及的URL走勢



新一代釣魚攻擊 (Phishing)

Quishing (QR Code)



Zishing (Zoom)



Vishing (Voice)



新一代釣魚攻擊 (Phishing)

Smishing (SMS)

商戶短訊



釣魚短訊



新一代釣魚攻擊 (Phishing)

SEO Poisoning (搜尋器優化中毒)



Google search results for "whatsapp download". The search bar shows "whatsapp download". Below the search bar, there are filters for "全部", "新聞", "影片", "圖片", "書籍", and "更多". The search results show approximately 3,450,000,000 results in 0.38 seconds. A red box highlights the top search result: "廣告 · https://www.whatspo.com/ whatsapp 中文版 - whatsapp 网页版". Below this, there is a link to "https://www.whatsapp.com/download" and "WhatsApp Download". A second red box highlights the text "廣告 · https://www.whatspo.com/ whatsapp 中文版 - whatsapp 网页版".



News article from Star Island titled "網民誤入假網站訂PHD Pizza 被盜用信用卡險失2.5萬元 結局超反轉". The article features a headline "盜亦有道？網民中伏入錯假網站叫外賣" and a sub-headline "信用卡被盜用 照收到Pizza 專家解構原因……". The image shows a pizza, a receipt, and a credit card. The article text includes: "騙徒手法層出不窮，不小心就很容易墜入陷阱。早前已有報道指騙徒會利用Google賣廣告置頂機制，偽冒商店網站，藉機盜用信用卡資料。近日又有一名網民中招，幸全身而回，更有驚人結局。"

新一代釣魚攻擊 (Phishing)

找出不同的地方:

A) `www.example.com`

B) `www.examp1e.com`

(小楷 l 與 1)

C) `www.example.com`

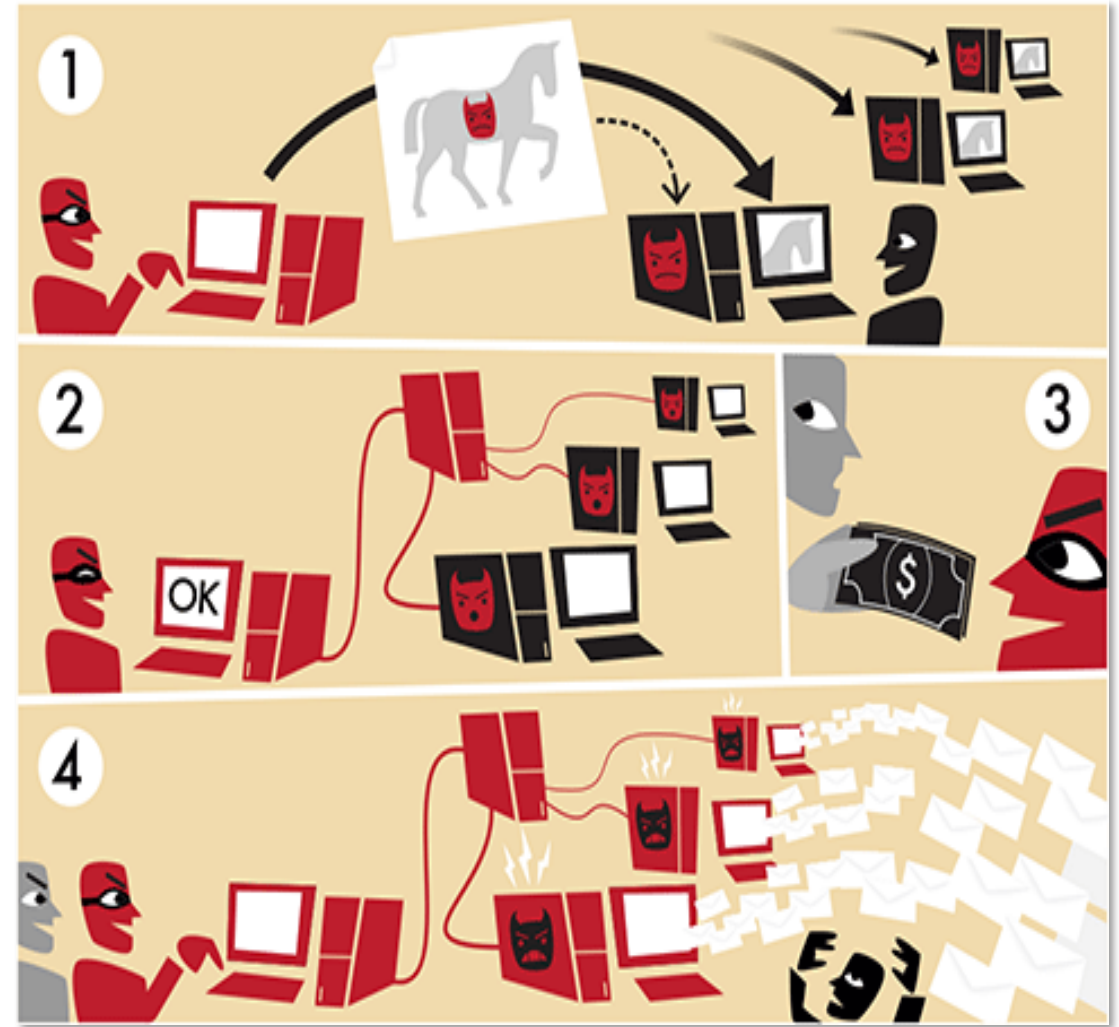
(“a” and “e” 西里爾字母)

Cyrillic Characters (西里爾字母)

А а	a as in father	К к	k as in class	Х х	h as in loch
Б б	b as in but	Л л	l as in love	Ц ц	ts as in its
В в	v as in van	М м	m as mother	Ч ч	ch as in chess
Г г	g as in get	Н н	n as in name	Ш ш	sh as in fish
Д д	d as in dress	О о	o as in bottle	Щ щ	shsh in fresh chat
Е е	ye as in yesterday	П п	p as in paper	Ъ ъ	"hard sign"
Ё ё	yo as in yonder	Р р	r as in error	Ы ы	i as in bill
Ж ж	zh as in measure	С с	s as in smile	Ь ь	"soft sign"
З з	z as in zoo	Т т	t as in ten	Э э	e as in bet
И и	ee as in meet	У у	u as in cool	Ю ю	yu in Yugoslavia
Й й	y as in toy	Ф ф	f as in farm	Я я	ya as in yard

殭屍網絡 (Botnet)

- 「bot」是「robot」的簡稱，加上「net」即是「機械人連結成的網絡」
- 裝置受惡意程式感染，被安裝「殭屍電腦程式」後會成為「殭屍電腦」，繼而受黑客控制，透過**指揮伺服器**（簡稱**C&C**或**C2 伺服器**），向殭屍電腦發出指令進行工作。
- 殭屍網絡一般由**數百部**，甚至**百萬部**裝置組成，這些裝置包括 PC、Mac、Linux 伺服器、家用路由器、智能手機等。



殭屍網絡如何運作 (圖片由 Tom-b 創作：
<http://commons.wikimedia.org/wiki/File:Botnet.svg>)

殭屍網絡 (Botnet)

現在閱讀
網絡安全 | 「911 S5」殭屍網絡破壞性有多大？ 影響全球近1900萬IP地址

網絡安全 | 「911 S5」殭屍網絡破壞性有多大？ 影響全球近1900萬IP地址

科技

撰文：梁巧恩

發布時間：2024/11/02 14:00



▲ 「911 S5」殭屍網絡自今年5月被發現，至今已影響全球近1900萬個IP地址。

ezone

香港網絡安全事故協調中心發呼籲 公眾宜嚴防殭屍網絡「911 S5」

| 梁家安 | 04-11-2024 08:26 |



惡意軟件(Malware - Malicious software)



- ❑ **勒索軟體 (Ransomware)** - 感染電腦並加密電腦上的重要檔案。一旦這些檔案被**加密**，勒索軟體業者就會要求付款以換取解密遺失檔案所需的**金鑰**
- ❑ **間諜軟體或資訊竊取程式** - **監視**電腦使用者的惡意軟體
- ❑ **木馬程式** - **偽裝**成其他東西的惡意軟體 - 此類惡意軟體試圖竊取線上帳戶的**憑證**，這些憑證可以授予其作者存取線上銀行帳戶和其他收入來源的**權限**
- ❑ **加密挖礦惡意軟體** - 軟體使用受感染電腦的**中央處理器資源**來解決這些問題，為惡意軟體營運商賺錢。在全球範圍內，加密挖礦惡意軟體佔**惡意軟體攻擊的 22%**

勒索軟體 (Ransomware)



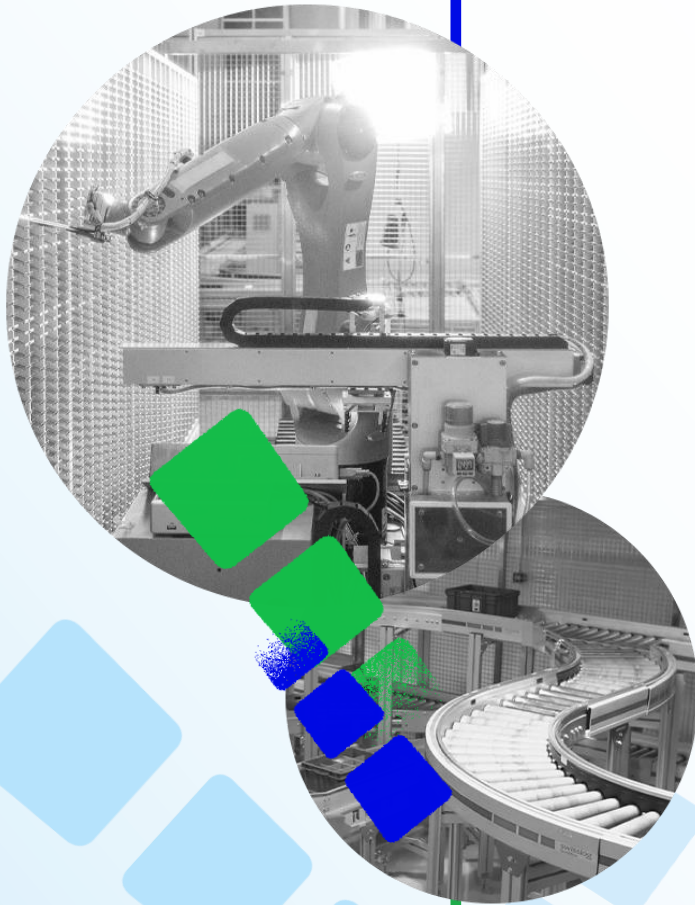
WannaCry (2017)



Lockbit (2019 – 2024)

木馬程式 (Trojan)






“

保安建議

”

超過一半的 網絡攻擊來自 網絡釣魚



投資過百萬元購買網絡安全
軟件及硬件



員工不慎按下釣魚電郵超連結

The server has infected by ransomware

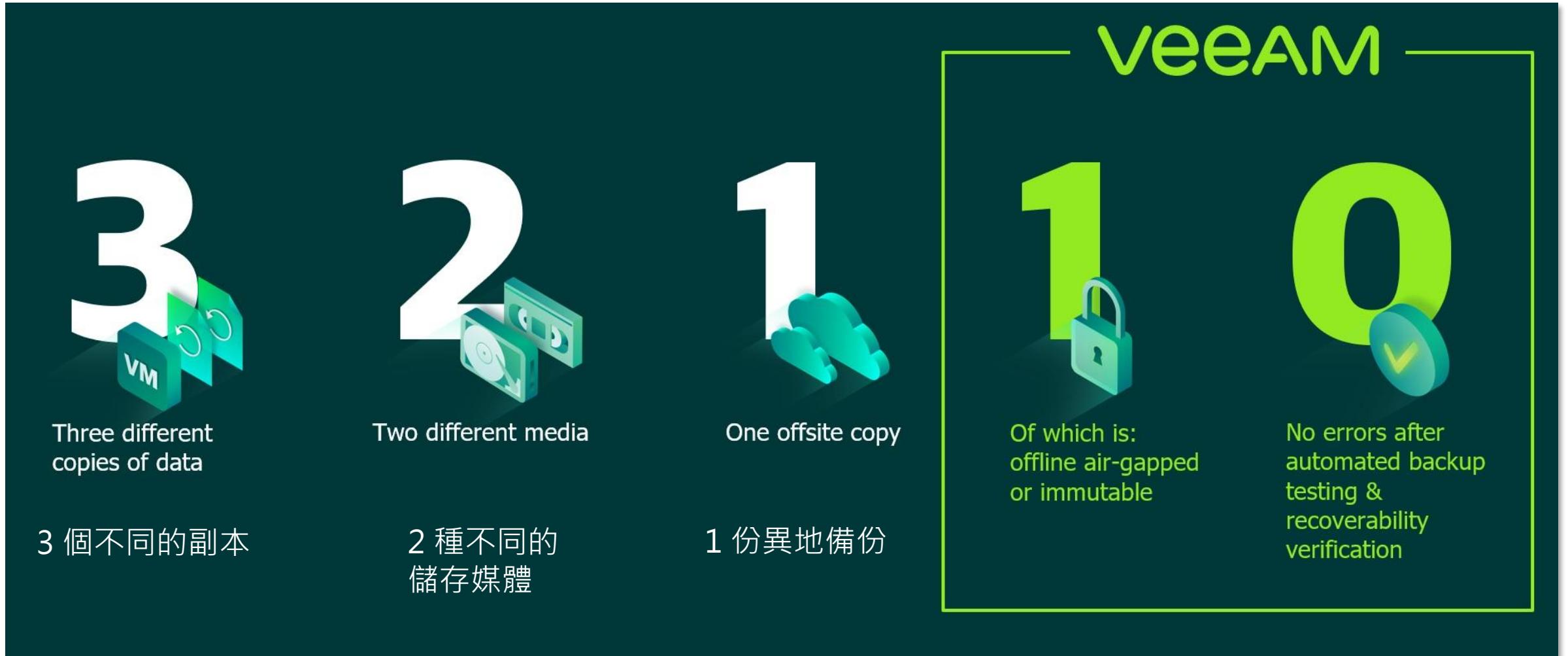


Where is backup?



On the server

備份原則: 3-2-1



Source: [veeam](https://www.veeam.com)



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



-Data sourced from [HowSecureismyPassword.net](https://howsecureismypassword.net)


軟件下載及更新



採取「零信任」 (Zero Trust) 態度

「永不信任，驗證為上」



UNITED 

STAR ALLIANCE 



Your device ran into a problem and needs to restart.
We're just collecting some error info, and then we'll
restart for you.

100% complete



For more information about this issue and possible fixes, visit
<https://www.apple.com/support/>

Open all 3 support pages, go to the bottom
of each page, scroll to the bottom, and
click the link.

Gates C70-C99  
Terminals A B  
United Club (C74)  

從網絡安全 (Cyber Security) 到網絡韌性 (Cyber Resilience)

提高警覺留意網絡安全風險，請訂閱或關注：

1. 免費安全公告和每月新聞通訊



2. 免費短訊(SMS)提醒



3. HKCERT 的社交媒體平臺 (例如 Facebook 、 LinkedIn 和 YouTube)



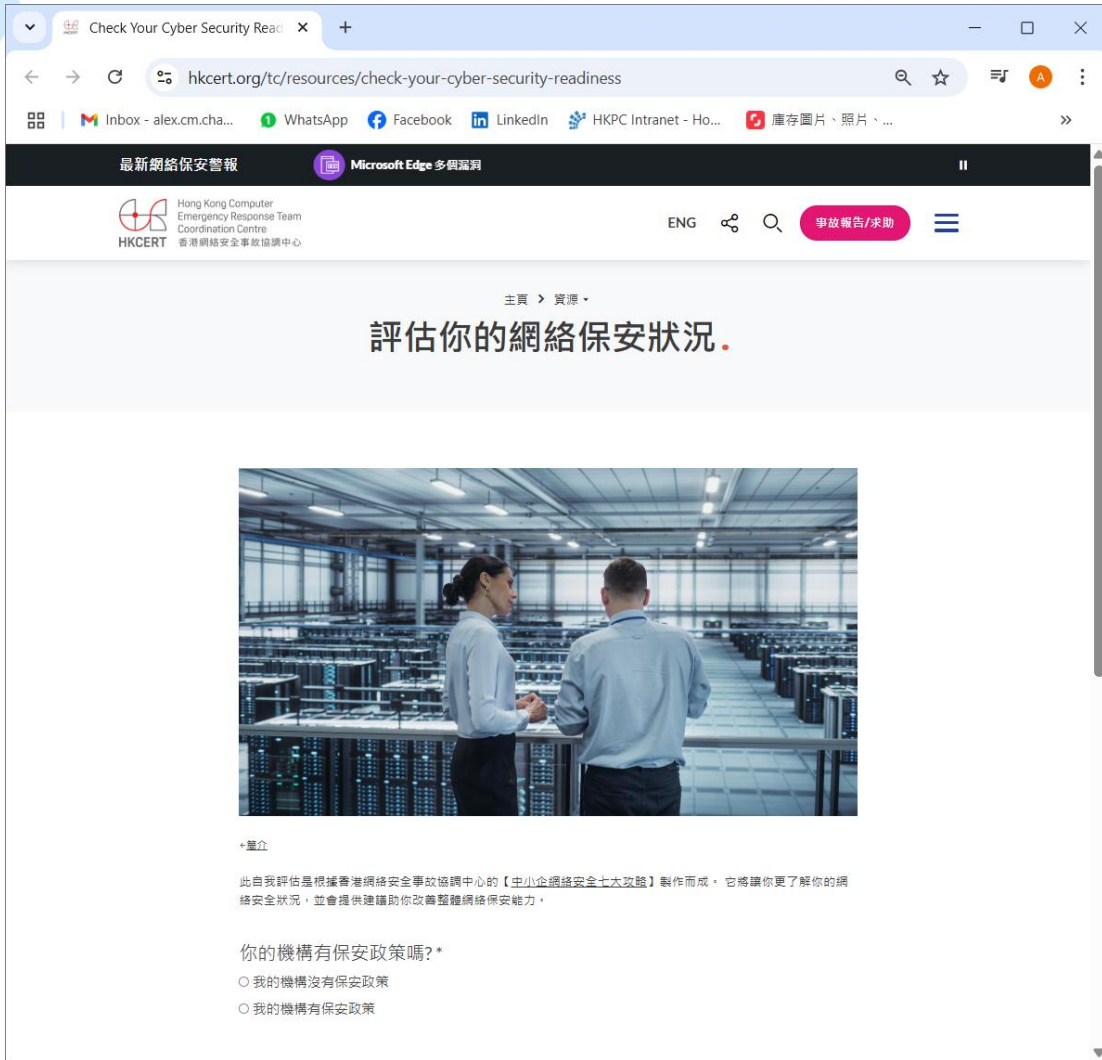
立即行動！

<https://www.hkcert.org/tc/form/subscribe/entry>

SUBSCRIBE



線上自我評估工具及中小企保安事故應變指南



防騙視伏器



**自動偵伏
舉報騙局**

蔡卓妍

鍾欣潼

下載「防騙視伏APP」

詳情即上 cyberdefender.hk



Scamometer+

下載防騙視伏APP

Download on the
App Store

GET IT ON
Google Play

EXPLORE IT ON
AppGallery



生產力局網絡安全框架



生產力局網絡安全培訓

(ISC)² - PROFESSIONAL SECURITY CERTIFICATION

- Certified in Cybersecurity (CC) Official Training
- Certified Cloud Security Professional (CCSP®) Official Training
- Certified Information Systems Security Professional (CISSP®) Official Training

KUNGFU SERIES

- Pentest "Kungfu" - Advanced Cyber Security Exploit Workshop
- Python "Kungfu" for Cyber Security Testing, Threat Intelligence and Automation
- Cyber Security Workshop : RED / BLUE Team Pentest Kungfu Series

EC-COUNCIL - ETHICAL HACKER SERIES

- Certified Ethical Hacker (CEH)
- Certified Ethical Hacker (CEH) & Practical

CHECK POINT SERIES (COMING SOON)

- Check Point Certified Security Administrator (CCSA)
- Check Point Certified Security Expert (CCSE)



ISO SERIES

- ISO/IEC 20000 Lead Auditor
- ISO/IEC 27005 Lead Risk Manager
- ISO/IEC 38500 IT Corporate Governance Manager
- ISO/IEC 38500 Lead IT Corporate Governance Manager
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27005 Lead Risk Manager

MOBILE SECURITY SERIES

- Practical EMM-MDM on Android Devices for better Security & Productivity
- Practical EMM-MDM on iOS Devices for better Security & Productivity
- Mobile Security for Android & iOS Devices Meets Productivity
- Better Mobile Security & Productivity for Android Devices
- Better Mobile Security & Productivity for Apple iOS Devices

CLOUD SERIES & SECURE CODING

- Securing Public Cloud Deployment
- Securing PaaS Cloud Deployment
- Building a Cyber Security, Cloud Protection and Privacy Framework
- Securing Your E-Commerce Web Application Against Cyber Threats
- Secure Coding and Application Security Workshop



Hong Kong Computer
Emergency Response Team
Coordination Centre
香港網絡安全事故協調中心

hkcert@hkcert.org
(852) 8105 6060



cybersec@hkpc.org
(852) 2788 5678



值得信賴的夥伴

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
Tel: +852 2788 5678 Whatsapp: +852 5283 4131
www.hkpc.org



謝謝

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
Tel: +852 2788 5678 Whatsapp: +852 5283 4131
www.hkpc.org