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


# 2025
# 網絡安全報告
# Cybersecurity Report

防騙視伏APP_Scameter+

網絡安全及科技罪案調查科
Cyber Security and Technology Crime Bureau
香港灣仔軍器廠街一號警察總部警政大樓
Arsenal House, Police Headquarters, No. 1 Arsenal Street, Wan Chai, Hong Kong

創新引領　護網守城

共築防線　賦能未來

Leading with Innovation

Securing the Cyberspace

Forging United Defence

Empowering the Future

# 目錄 TABLE OF CONTENTS

# 序言
# Foreword

維護本港的網絡公共安全，是香港警務處網絡安全及科技罪案調查科（網罪科）肩負的使命，亦是維護國家安全和社會穩定的重要工作。本人謹向網罪科團隊及各界持份者致以由衷感謝，感謝大家過去一年的鼎力支持與緊密合作。今年，網罪科再次發佈新一份《網絡安全報告2025》，回顧2025年香港在網絡安全領域的挑戰與成果，並前瞻未來的機遇與發展方向。

Safeguarding Hong Kong's online public safety is the vital mission of the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF), and a critical task in maintaining national security and social stability. I would like to express my heartfelt gratitude to the CSTCB team and all stakeholders for their ongoing support and cooperation over the past year. This year, CSTCB released the Cybersecurity Report 2025, reviewing the challenges and achievements in Hong Kong's cybersecurity landscape over the past year, while looking ahead to future opportunities and strategic priorities.

2025年，全球網絡犯罪形勢依然嚴峻。根據網絡安全機構估算，2025年網絡犯罪造成的全球經濟損失高達萬億級美元，且仍在每年繼續上升。香港作為國際金融及創新科技樞紐，無可避免地成為網絡犯罪的目標之一。隨著人工智能技術被應用於網絡攻擊，全球網絡安全風險正加速向自動化、跨領域及高度複雜化方向發展。去年，網罪科網絡安全中心共處理並分析了超過3 500萬項網絡威脅情報，其中針對香港的攻擊超過154萬項，同比升幅分別達4成及2.4倍，反映出網絡威脅的規模與複雜性持續攀升。儘管如此，憑藉我們持續高效的網絡安全防禦機制以及與各持份者的緊密網絡安全生態協作，使香港繼續是世界上其中一個最安全及穩定的網絡環境。即使網罪科收集的網絡威脅情報持續上升，2025年香港並未有必要服務因網絡攻擊而中斷。

In 2025, the global cybercrime landscape remained severe. According to estimates from cybersecurity organisations, cybercrime resulted in global economic losses reaching trillion of dollars in 2025, a figure that continues to rise annually. As an international financial and innovation hub, Hong Kong inevitably remains one of the targets for cybercriminals. With AI increasingly being applied to cyberattacks, global cybersecurity risks are accelerating towards greater automation, cross-domain impact, and sophistication. Throughout the year, CSTCB's Cyber Security Centre (CSC) processed and analysed more than 35 million pieces of cyber threat intelligence, of which over 1.54 million were attacks directed at Hong Kong, representing year-on-year increases of approximately 40% and 2.4 times respectively. The figures underscore the growing scale and sophistication of cyber threats. Nevertheless, through our consistently effective cybersecurity defence mechanisms and close cybersecurity ecosystem collaboration with stakeholders, Hong Kong continues to maintain one of the safest and most stable cyber environments in the world. Despite the continued increase in cyber threat intelligence collected by CSTCB, no essential services in Hong Kong were disrupted by cyberattacks in 2025.

在國際合作方面，2025年是香港警隊與國際刑警組織及多個執法機構深化協作的一年。去年，我除了擔任國際刑警組織亞洲及南太平洋科技罪案聯合行動工作組副主席，亦獲選為國際刑警組織網絡罪案專家組主席，持續深化情報交流及提升跨境聯合行動能力。我帶領網罪科團隊積極參與了多項國際會議，包括6月於法國里昂舉行的國際刑警組織網絡罪案專家組周年會議、7月於越南河內舉行的國際刑警組織亞洲及南太平洋科技罪案聯合行動工作組會議，以及8月於南韓首爾舉行的第十五屆國際刑警組織網絡罪案首長級工作坊及國際網絡罪案應變研討會。此外，網罪科亦成功舉辦了第十屆數碼法理鑑證專家小組會議及第二屆國際數碼鑑證挑戰賽，進一步鞏固香港作為國際數碼法證專業交流樞紐的地位。

In terms of international cooperation, 2025 was a year of deepening synergy between the HKPF, INTERPOL, and various law enforcement agencies. Last year, apart from serving as the Vice-chairperson of the INTERPOL Asia and South Pacific Joint Operations on Cybercrime Working Group, I was also elected chairperson of the INTERPOL Cybercrime Expert Group (CyberEX). We actively participated in several international conferences, including the INTERPOL CyberEX meeting in Lyon, France, in June; the INTERPOL Asia and South Pacific Working Group Meeting on Cybercrime for Heads of Units in Hanoi, Vietnam, in July; and the 15th INTERPOL Cybercrime Directors' Workshop and the International Symposium on Cybercrime Response (ISCR) in Seoul, South Korea, in August. Furthermore, CSTCB successfully hosted the 10th Digital Forensic Expert Group (DFEG) Meeting and the 2nd International Digital Forensics Challenge (IDFC), further consolidating Hong Kong's position as an international hub for digital forensic professionals.

為進一步提升香港的整體網絡防禦能力，網罪科積極利用創新科技加強情報與數據交流能力，其中包括於2025年全面升級「防騙視伏器+」平台，新增人工智能驅動的風險評估功能，為市民提供更快速、準確的詐騙預警。同時，網罪科亦深化了與金融界的合作，將「防騙視伏器」數據融入開戶程序與交易監察流程，協助識別可疑賬戶，推動反詐騙工作的全面化。另外，網罪科持續擴展「網絡安全行動中心聯盟」的規模，匯聚航空運輸、銀行與金融服務、通訊、能源、政府、醫療保健服務、陸路運輸、海事、公共事業、廣播服務等大型及重要基礎設施，利用人工智能驅動的大數據互聯互通平台，促進跨行業網絡威脅情報共享。

To further enhance Hong Kong's overall cyber defence capabilities, CSTCB has leveraged innovation and technology to strengthen intelligence and data sharing. In 2025, we comprehensively upgraded the Scameter+ platform, introducing AI-driven risk assessment features to provide citizens with faster and more accurate fraud alerts. Also, we deepened our collaboration with the financial sector by integrating Scameter data into account opening and transaction monitoring processes to help identify suspicious accounts and promote a holistic approach to anti-deception work. Furthermore, CSTCB continued to expand the Security Operation Centre Alliance (SOCA), bringing together major and critical infrastructure (CI) sectors — including air transport, banking & financial services, communications, energy, government, healthcare services, land transport, maritime, public utilities, and broadcasting services—while leveraging an AI-driven big data interconnection platform to facilitate cross-industry cyber threat intelligence sharing.

網絡威脅日益趨向自動化與跨領域化，單一機構的力量已不足以應對全球性的安全挑戰。為此，網罪科積極深化公私營夥伴關係，與各界攜手共建互信的網絡安全生態。我們透過「網絡安全特別行動小組」強化與業界的即時情報及專業知識共享；而原名為「科技罪案警政顧問小組」的架構亦於 2025 年更名為「智慧警政顧問小組」，匯聚專家智慧，為數碼警務的長遠規劃提供策略建議。此外，透過舉辦「網絡安全精英嘉許計劃」，我們向64名得獎者及19間機構頒發獎項，表揚他們在網絡安全方面的卓越成就，藉此激發業界力求創新，鼓勵以科技預防網絡攻擊，持續提升本港的網絡安全水平。

As cyber threats become increasingly automated and cross-domain, the strength of a single organisation is no longer sufficient to counter global security challenges. To this end, CSTCB has actively deepened its Public-Private Partnerships (PPP) to build a trusted cybersecurity ecosystem. Through the Cyber Security Action Task Force (CSATF), we have strengthened the real-time sharing of intelligence and expertise with the industry. The "Cybercrime Policing Advisory Panel" was also officially renamed the Smart Policing Advisory Panel (SPAP) in March 2025, gathering expert wisdom to provide strategic advice for the long-term planning of digital policing. Furthermore, through the Cyber Security Professional Awards (CSPA), we commended 64 winners and 19 organisations for their outstanding achievement in cybersecurity, inspiring industry innovation and encouraging the use of technology to prevent cyberattacks, thereby continuously raising the level of cybersecurity in Hong Kong.

此外，為提升整體網絡安全實踐能力，網罪科成功舉辦了多項大型活動及演練，包括「網絡攻防精英培訓暨攻防大賽」、「網絡安全多元創新論壇」及「跨部門網絡安全演習」，吸引了來自公私營機構、學界及業界的廣泛參與。透過「守網聯盟」，我們匯聚超過130個政府部門、公營機構、非牟利機構及大型企業聯手推廣防騙宣傳教育。於2025年，更聯同教育局及數字政策辦公室進一步推出「守網聯盟遊戲卡」，在全港中小學推廣網絡安全教育，透過「數碼素養」導師教材套及遊戲化的方式，讓青少年自小培養數碼素養，同時展現我們透過社區協作、以賦能為本的警政策略。

Moreover, to enhance overall cybersecurity practical capabilities, CSTCB successfully organised several large-scale events and exercises, including the Cyber Attack and Defence Elite Training cum Tournament (CADET), the Cybersecurity & Diverse Innovation Symposium, and the Inter-departmental Cyber Security Drill, attracting wide participation from public and private sectors, academia, and the industry. Through the "CyberDefenders' Alliance", we have brought together more than 130 government departments, public bodies, non-profit organisations and major corporations to jointly promote anti-scam publicity and education. In collaboration with the Education Bureau and the Digital Policy Office, we further launched the "CyberDefenders' Alliance Card Game" in 2025 to promote cybersecurity education in primary and secondary schools across Hong Kong. Through the "digital literacy" teaching kits for instructors and a gamified approach, we aim to nurture digital literacy among youths from an early age, while demonstrating our policing strategy based on community collaboration and empowerment.

來年，網罪科將設立「智慧警政聯合人工智能實驗室」，進駐數碼港人工智能超算中心，與多家科企共同研發人工智能應用項目，繼續以創新科技為主導，配合超算設備的高速發展，全方位推動香港網絡安全生態的發展，致力為香港的數碼轉型及智慧城市建設築起堅固的網絡安全防線。最後，本人期望未來能繼續與各界攜手合作，共同維護香港的網絡安全，為社會的長遠發展奠定穩固基石。

In the coming year, CSTCB will establish the "Smart Policing Joint AI Lab" at the Cyberport's Artificial Intelligence Supercomputing Centre, working with multiple technology companies to jointly research and develop AI application projects. Remaining innovation-led and harnessing the rapid advancement of supercomputing capabilities, we will continue to drive the comprehensive development of Hong Kong's cybersecurity ecosystem and build a solid cybersecurity defence for the city's digital transformation and smart city development. Lastly, I look forward to continuing our partnership to jointly maintain the security and stability of Hong Kong's cyberspace, laying a solid foundation for the long-term development of our society.


林焯豪
Raymond LAM
香港警務處
網絡安全及科技罪案調查科總警司
Chief Superintendent of Police
Cyber Security and Technology Crime Bureau
Hong Kong Police Force

# 專業見解
# Key Insights

國際刑警組織與香港警務處攜手打擊全球網絡犯罪。

INTERPOL and Hong Kong Police Force unite to combat cybercrime worldwide.

INTERPOL

Mr. Neal JETTON
國際刑警組織網絡犯罪主管
Director of Cybercrime, INTERPOL

張宜偉先生, JP
Mr. CHEUNG Yee Wai, Daniel, JP
現任署理數字政策專員
the incumbent Commissioner for Digital Policy (Acting)

中華人民共和國香港特別行政區政府
數字政策辦公室
Digital Policy Office
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

前沿科技快速發展，供應鏈越趨複雜，網絡安全防禦面臨全新挑戰。政府、業界、學界必須攜手合作強化網路安全生態圈，確保科技持續成為經濟增長動力，而非風險來源。

The rapid development of cutting-edge technology and the increasing complexity of supply chains present new challenges to cybersecurity defences. Governments, industries, and academia must collaborate to fortify the cybersecurity ecosystem, ensuring that technology remains a driver of economic growth rather than a source of risk.

自2026年起，香港關鍵基礎設施的安全從「認知」走向「實踐」，強調企業管治、可落實標準及公私營合作。透過持續提升人員、流程及科技，並加強供應商與合作夥伴的安全責任，方可建立網絡韌性。

From 2026, Hong Kong's critical infrastructure security shifts from awareness to action, emphasising corporate governance, actionable standards, and public-private collaboration. Cyber resilience requires continuous improvement in people, processes, and technology, enhancing security responsibilities of suppliers and partners.

中華人民共和國香港特別行政區政府
保安局關鍵基礎設施(電腦系統安全)專員辦公室
Office of the Commissioner of Critical Infrastructure (Computer-system Security), Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

陳永安先生
Mr. Francis CHAN Wing-on
關鍵基礎設施(電腦系統安全)專員
Commissioner of Critical Infrastructure (Computer- system Security)

畢堅文先生, MH
Mr. Mohamed BUTT, MH
香港生產力促進局總裁
Executive Director, Hong Kong Productivity Council (HKPC)

人工智能雖加速了創新步伐，但也正以讓人措手不及的速度，徹底改寫全球網絡安全風險的面貌。

AI is accelerating innovation — but it is also reshaping the global cyber risk landscape faster than many are prepared for.

以零信任築牢防線，落實「系統、政策、人員」三重防護。

Empowering resilient security with Zero Trust across systems, policies, and people

hkirc

黃家偉工程師
Ir Wilson WONG
香港互聯網註冊管理有限公司行政總裁
CEO, Hong Kong Internet Registration Corporation Limited (HKIRC)

網絡安全人人有責，政府、企業、民眾攜手合作，完善政策和標準、落實措施和演練、培養人才和意識，方能防禦不斷演變的網絡攻擊，維護社會穩定及保障民眾安全。

Cybersecurity is a collective responsibility that demands a unified front from the government, enterprises, and the public. By collaborating to refine policies and standards, execute rigorous measures and drills, cultivate talent and foster awareness, we can mitigate the ever-changing cyberattacks, thereby maintaining social stability and protecting the lives of citizens.

數碼港 Cyberport

鄭松岩博士
Dr. Rocky CHENG
數碼港行政總裁
CEO, Cyberport

顧榮輝教授
Professor GU Ronghui
CertiK聯合創辦人
Co-founder, CertiK

CERTIK

網絡安全正進入一個新階段：技術韌性必須與監管機制、問責制度及跨領域協作並重。

Cybersecurity is entering a phase where technical resilience must be matched by governance, accountability, and cross-sector coordination.

楊霞教授
Professor YANG Xia
Beosin創辦人
Founder, Beosin

BEOSIN
Web3 Security & Compliance

人工智能與區塊鏈加速數字經濟發展，但同時加劇網絡犯罪，需要先進技術與全球協作，以提升Web3生態的安全性及應對新興威脅。

AI and blockchain accelerate the digital economy but also intensify cybercrime, requiring advanced technologies and global collaboration to enhance Web3 ecosystem security and address emerging threats.

通過資訊科技治理、協作及專業發展建立集體防禦機制，方能有效預防、偵測及應對新興網絡威脅。

A unified approach through governance, collaboration, and professional development is pivotal to preventing, detecting, and neutralising these emerging cyber threats.

ISACA
China Hong Kong Chapter

朱偉年博士
Dr. Welland CHU
國際信息系統審計協會(中國香港分會)會長
President, ISACA China Hong Kong Chapter

蕭子豪先生
Mr. XIAO Zihao
瑞萊智慧科技聯合創辦人及技術總監
Co-founder & CTO, RealAI

RealAI 瑞萊智慧

在AI快速發展的背景下，AI的可控和安全是迫在眉睫的問題。

Amid rapid AI advancement, AI controllability and safety are pressing concerns.


# 關於本報告
# About the Report

本報告旨在為網絡安全從業者及日常需落實網絡安全措施的資訊科技人員提供實用參考。針對企業高層管理人員，報告提出具操作性的建議，協助其制定更周詳的決策，以強化機構整體防護能力。儘管報告內容技術性較強，公眾仍可透過此報告掌握基礎防護建議，培養個人網絡安全意識與良好習慣，從而有效保障個人及網絡環境的安全。

This report offers practical insights primarily for cybersecurity practitioners and IT professionals implementing cybersecurity measures in their daily operations. For corporate senior management, it provides actionable recommendations to aid in making informed decisions to strengthen organisational defences. While technically oriented, members of the public can access basic protective advice through this annual report, enhance their personal cybersecurity awareness and cultivate good habits, thereby effectively protecting their personal information and online safety.

# 目標
## Objectives

本報告從警務政策角度闡述網絡安全工作，旨在提升公眾、網絡安全專才等各界人士及機構的網絡安全意識與防禦能力。透過結合警方行動、源自全球及本地的網絡威脅情報，以及來自網絡安全領域合作夥伴的貢獻，網罪科致力提供對香港網絡安全威脅形勢的全面概述，並給予可行建議，協助各持份者加強網絡防護，保障資訊科技系統、基礎設施及公共服務，以強化整體網絡安全。

The Cybersecurity Report addresses cybersecurity initiatives from a policing perspective. The report aims to raise cybersecurity awareness and enhance cyber defence capability across individuals and organisations, from the general public to cybersecurity professionals. Drawing on operational findings, cyber threat intelligence from global and local sources, and contributions from cybersecurity partners, CSTCB seeks to provide a comprehensive overview of Hong Kong's cybersecurity threat landscape, as well as actionable insights that assist stakeholders in strengthening cyber protection measures, safeguarding information technology systems, critical infrastructures and public services, and reinforcing the overall cybersecurity posture.

# 致謝
## Acknowledgements

本年報由網罪科撰寫，並獲得以下合作夥伴的寶貴貢獻（按照英文字母順序排列）：

This report was written by CSTCB with invaluable contribution from the following partner organisations (listed in alphabetical order):-

- 阿里雲 Alibaba Cloud
- Beosin
- CertiK
- 中國移動香港 China Mobile Hong Kong (CMHK)
- 數碼港 Cyberport
- 數字政策辦公室 Digital Policy Office (DPO)
- Group-IB
- 香港互聯網註冊管理有限公司
  Hong Kong Internet Registration Corporation Limited (HKIRC)
- 香港生產力促進局
  Hong Kong Productivity Council (HKPC)
- 國際刑警組織 INTERPOL
- 國際信息系統審計協會中國香港分會
  ISACA China Hong Kong Chapter
- 卡巴斯基 Kaspersky
- 關鍵基礎設施（電腦系統安全）專員辦公室
  Office of the Commissioner of Critical Infrastructure (Computer-system Security)
- 瑞萊智慧 RealAI
- 深信服 Sangfor
- 微步在線 ThreatBook

中華人民共和國香港特別行政區政府
數字政策辦公室
Digital Policy Office
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

中華人民共和國香港特別行政區政府
保安局關鍵基礎設施（電腦系統安全）專員辦公室
Office of the Commissioner of Critical Infrastructure (Computer-system Security), Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

# 免責聲明
## Disclaimer

本報告提供的資訊僅供參考。報告中對威脅者的描述僅基於技術分析，不涉及政治歸因。香港特別行政區政府及網罪科對本報告內任何不準確、錯誤或遺漏，以及因使用本報告資訊或根據該資訊提供建議而引致的任何損失、行動或不作為，概不負責。

The information provided in this report is for reference only. The descriptions of threat actors in this report are based solely on technical analysis and do not constitute political attribution. The Government of the Hong Kong Special Administrative Region (HKSARG) and CSTCB accept no liability for any inaccuracies, errors or omissions in this report, or for any loss, action or inaction arising from the use of, or from advice based on, any information therein.

本報告得以完成，有賴各方攜手合作。

Their collaborative efforts were instrumental in making this Report possible.

# 2025年
# 網絡安全趨勢
# CYBERSECURITY TREND IN 2025

網絡威脅情報分析
Cyber Threat Intelligence Analysis

2025年網絡安全挑戰
Cybersecurity Challenges in 2025

針對重要基礎設施的網絡安全挑戰
Cybersecurity Challenges faced by Critical Infrastructures

網絡安全建議
Cybersecurity Mitigations

# 概述
## Overview

2025年，網絡攻擊越趨頻繁，威脅者的技術亦不斷演變。據估計，2025年網絡犯罪造成的全球經濟損失估計高達10.5萬億美元，年增長率接近15%[1]。

自2015年成立以來，網罪科一直採取多維度的綜合策略來守護香港的網絡安全。除了進行刑事調查以打擊罪案外，網罪科亦積極蒐集與共享網絡威脅情報以維護重要基礎設施的系統安全，並推動各類演練及教育活動以加深社會各界的網安意識。

為了精準掌握香港整體的網絡威脅態勢，網罪科致力於分析多元化的數據來源。這包括整合開源情報、專屬威脅情報源、前沿技術監控系統，並結合強大的專業合作夥伴網絡，以提升對潛在風險的預見能力。

In 2025, cyberattacks became increasingly frequent, while the techniques employed by threat actors also evolved. The estimated annual global economic loss attributed to cybercrime was US$10.5 trillion in 2025, reflecting an annual increase of nearly 15%[1].

Since its inception in 2015, CSTCB has adopted a comprehensive, multi-dimensional strategy to protect Hong Kong's digital landscape. Beyond traditional criminal investigations, CSTCB also focuses on cultivating and sharing proactive threat intelligence, ensuring the resilience of critical infrastructures, and spearheading drills and educational initiatives to foster a culture of cybersecurity awareness.

To achieve high visibility of the local threat environment, CSTCB utilises a multi-layered analysis of diverse data streams. This includes integrating open-source intelligence (OSINT), proprietary threat feeds, and cutting-edge monitoring systems alongside an extensive network of strategic partnerships, to enhance our ability to anticipate potential risks.

網罪科轄下的網絡安全中心全年無間斷運作，提供24小時的威脅監控與支援。中心除了透過情報收集來分析網絡攻擊手法，亦負責全天候監察重要基礎設施系統的正常運作，並隨時提供不同等級的網絡防禦與行動支援。

網罪科轄下的網絡安全行動中心聯盟旨在建立制度化的協作平台，推動各重要基礎設施安全行動中心之間的威脅情報共享與協同應對。透過自動化平台及威脅關聯分析，形成跨機構協作，並與網絡安全特別行動小組內的多個國際網絡安全組織緊密配合，確保新興威脅能被迅速識別及處理。此舉旨在培養持續情報共享文化，並將情報轉化為可行動的措施，全面提升防禦韌性。

The CSC, operating round-the-clock throughout the year, serves as our frontline for threat monitoring and support. In addition to collecting and analysing intelligence to study cyberattack methodologies, the Centre also provides constant operational support and multi-level defensive assistance to ensure the stable operation of critical infrastructure systems.

Furthermore, SOCA serves as a structured platform to promote threat intelligence sharing and coordinated response among Security Operation Centres of critical infrastructures. By leveraging automated platforms and threat correlation analysis, SOCA facilitates cross-agency collaboration and works in close partnership with multiple international cybersecurity organisations within CSATF. This ensures the rapid identification and mitigation of emerging threats, fosters a culture of continuous intelligence sharing, and transforms intelligence into actionable measures, thereby comprehensively enhancing defensive resilience.

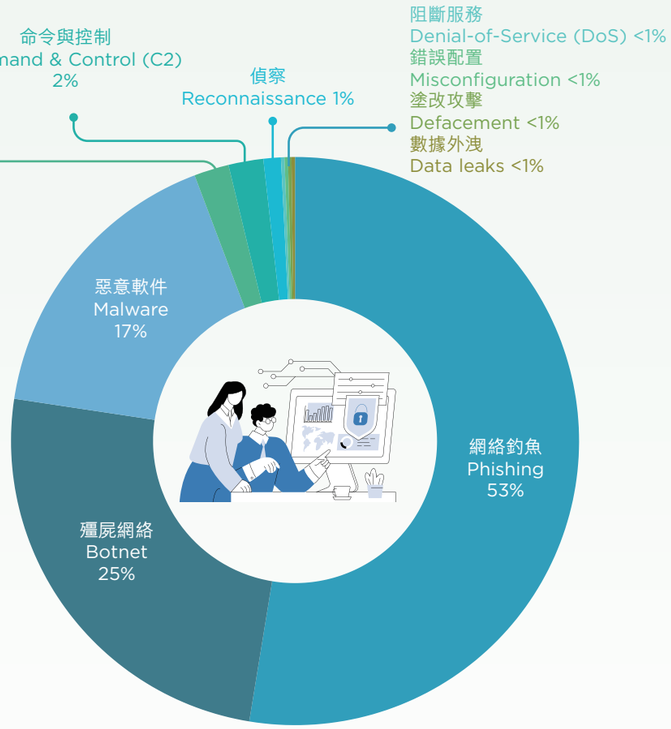
# 網絡威脅情報分析
## Cyber Threat Intelligence Analysis

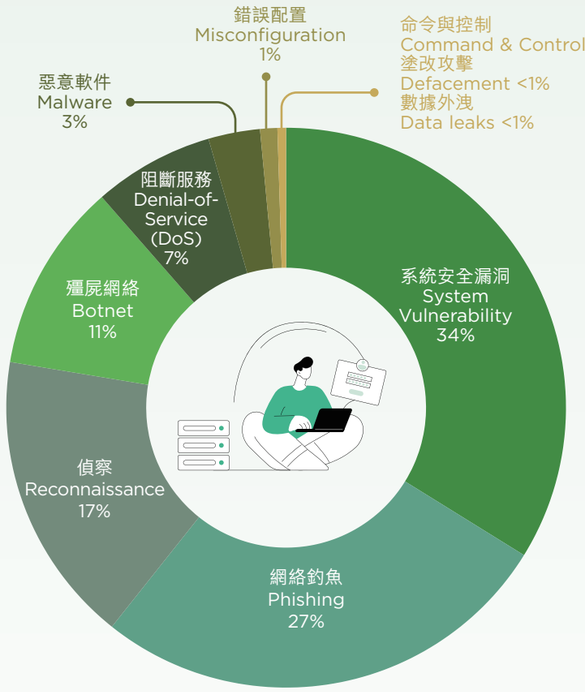
2025年，網罪科共分析逾3 500萬項網絡威脅情報，較2024年增加逾千萬項，反映威脅環境日益複雜。相關數據及分析成果亦成為本年度報告的重要依據。

In 2025, CSTCB analysed over 35 million pieces of cyber threat intelligence, representing an increase of over 10 million compared with 2024. This growth underscores the escalating complexity of the cyber threat landscape. The relevant data and analytical findings serve as a crucial basis for this annual report.

2025年
網罪科處理的網絡威脅情報
Cyber Threat Intelligence Processed by CSTCB in 2025

**35,000,000+**




2025年
針對香港的網絡威脅情報
Cyber Threat Intelligence Targeting Hong Kong in 2025

**1,540,000+**

其中，網罪科發現超過154萬項針對香港的網絡威脅情報，主要與系統安全漏洞、網絡釣魚及偵察活動有關，三者分別佔所有香港網絡威脅情報的34%、27%及17%。

In particular, CSTCB detected over 1.54 million pieces of cyber threat intelligence specifically targeting Hong Kong, primarily related to system vulnerabilities, phishing, and reconnaissance activities, which accounted for 34%, 27%, and 17% of all cyber threat intelligence targeting Hong Kong respectively.

[1] Cybersecurity Ventures. (2025, December 11). 2025 cybersecurity almanac: 100 facts, figures, predictions and statistics. Retrieved from https://cybersecurityventures.com/cybersecurity-almanac-2025/

## 系統安全漏洞 System Vulnerability

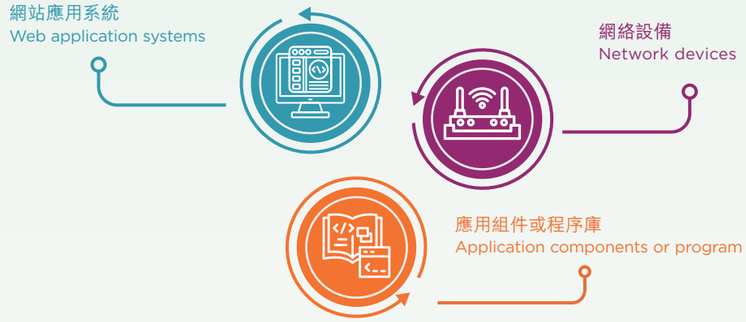
2025年，網罪科共收集約52.4萬項針對本地機構系統安全漏洞的情報，佔針對香港的網絡威脅情報的34%。我們研判，攻擊者正持續嘗試利用軟件、硬件或流程中的固有弱點或缺陷，在未經授權的情況下接達本地機構的電腦系統，以作進一步攻擊。

In 2025, CSTCB has collected about 524,000 pieces of threat intelligence targeting system vulnerabilities within local institutions, representing 34% of cyber threat intelligence targeting Hong Kong. We assess that attackers are persistently attempting to exploit inherent weaknesses or flaws in software, hardware, or processes to gain unauthorised access to the computer systems of local institutions for further attacks.

針對
本地機構系統
安全漏洞的網絡威脅情報
Cyber threat intelligence targeting system vulnerabilities with in local institutions
**524,000+**

佔針對香港
的網絡威脅情報
**34%**
of the cyber threat intelligence targeting Hong Kong


經深入分析網絡威脅情報後發現，攻擊者最常鎖定的三類目標分別是:
Upon in-depth analysis of cyber threat intelligence, we found that the most frequently targeted categories were:




當中攻擊者多數利用CVSS評分9.0以上的遠端執行程式碼漏洞。
where the most observed attacks involved remote code execution (RCE) vulnerabilities with CVSS scores above 9.0.

在網站應用系統方面，攻擊者主要針對內容管理系統，利用公開漏洞庫中的攻擊載荷進行自動化大規模攻擊。虛擬私有網絡（VPN）閘道和防火牆是第二大攻擊目標，尤其針對廠商披露的認證繞過和遠端執行程式碼漏洞。此外，攻擊者也會利用如Log4j、pyLoad等過時或存在漏洞的函數庫，以取得底層系統的控制權。

值得關注的是，威脅者將新發現漏洞轉化為攻擊武器的速度顯著加快，迫使防禦方必須加速修補漏洞。根據網絡安全公司的威脅情報分析，系統安全漏洞從披露到被實際利用的「漏洞利用時間」已大幅縮短。甚至在修補程式發布前，攻擊者就可能已經利用該漏洞入侵未及時修補的系統[2]。

Within the web application system, attackers mainly targeted Content Management Systems (CMS), using exploit payloads from public repositories to automate large-scale attacks. Network devices were the second major focus, particularly Virtual Private Network (VPN) gateways and firewalls affected by authentication bypass and Remote Code Execution (RCE) flaws disclosed by major vendors. Attackers also exploited vulnerable or outdated libraries and components, such as Log4j and pyLoad, to gain control of underlying systems.

It is noteworthy that the speed at which threat actors transform newly discovered vulnerabilities into offensive weapons has accelerated significantly, forcing defenders to speed up patching system vulnerabilities. According to threat intelligence analysis by a cybersecurity company, the "time-to-exploit"—the period from the disclosure of a system vulnerability to its actual exploitation—has been significantly shortened. Even before a patch is released, attackers may already exploit the vulnerability to intrude unpatched systems[2].

[2] Kutscher, J. (2026, March 24). M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/mtrends-2026



## 網絡釣魚 Phishing

2025年，網罪科偵測到超過42.1萬項與網絡釣魚相關的本地網絡威脅情報，佔針對香港的網絡威脅情報的27%。經分析後，我們發現最常被濫用作網絡釣魚的網站類型包括：即時通訊軟件、網上二手交易平台、網上付款平台、物流服務平台、網上銀行、社交媒體及政府部門繳費服務。攻擊者利用網絡釣魚進行兩種類型的攻擊：一種是以詐騙、盜取受害者金錢為目的；另一種則以盜取受害人的網上身份，以進行後續的詐騙或網絡入侵活動。

In 2025, CSTCB detected over 421,000 pieces of phishing-related local cyber threat intelligence, representing 27% of the cyber threat intelligence targeting Hong Kong. Upon analysis, we identified that the most commonly spoofed platforms in phishing attacks included instant messaging applications, online second-hand trading platforms, online payment platforms, logistics service platforms, online banking services, social media platforms, and government bill payment services. Attackers leveraged phishing to carry out two types of attacks: one aimed at defrauding and stealing money from victims, and the other aimed at stealing victims' online identities to facilitate further fraud or cyber intrusion activities.

網絡釣魚相關的
網絡威脅情報
Phishing-related cyber threat intelligence
**421,000+**

佔針對香港
的網絡威脅情報
**27%**
of the cyber threat intelligence targeting Hong Kong

最常被濫用作網絡釣魚的網站
The most commonly spoofed platforms in phishing attacks


以即時通訊軟件平台為例，攻擊者會透過短訊、電郵或搜尋器投毒的方式，廣泛散播釣魚網站。受害人被引導輸入其電話號碼，然後掃瞄釣魚網站上的二維碼，或輸入與其帳號綁定的配對代碼。一旦受害人授權配對，其即時通訊軟件帳戶便可能在不知不覺中被騎劫，讓攻擊者可以冒充其身份向其他聯絡人騙取金錢，或從聊天記錄中竊取敏感的個人及財務資訊。

隨著我們在網絡威脅情報收集方面的能力不斷提升，網罪科能夠及時偵測到用於網絡釣魚攻擊的惡意互聯網規約（IP）地址、劃一資源定位址（URL）及域名，並利用人工智能對相關惡意IP地址或域名進行反向檢查及關聯分析，自動化地發現更多附屬釣魚網站，再迅速採取行動移除這些釣魚網站。2025年所偵測到80%的釣魚網站存活期不超過一天，反映我們的偵測及應對機制運作成效顯著。

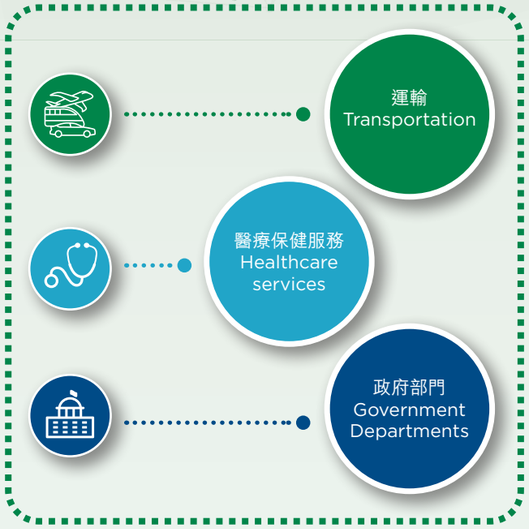
Taking instant messaging platforms as an example, attackers disseminated phishing websites extensively through SMS messages, emails, or search engine poisoning. Victims were lured to enter their phone numbers and then scan a QR code displayed on the phishing website, or enter a linking code tied to their accounts. Once the victims authorised the linking, their instant messaging account would be hijacked without their knowledge, allowing the attacker to impersonate them to defraud their contacts of money or to extract sensitive personal and financial information from their chat histories.

With our enhanced capability in cyber threat intelligence cultivation, CSTCB can detect malicious IP addresses, Uniform Resource Locators (URLs) and domains used for phishing attacks in a timely manner, leverage AI to conduct reverse lookups and correlation analysis on the relevant malicious IP addresses or domains, automatically identifying more associated phishing websites, and take prompt action to take down these phishing websites. In 2025, 80% of these phishing websites detected remained active for no more than one day, reflecting the significant effectiveness of our detection and response mechanisms.

## 偵察活動
## Reconnaissance Activities

2025年，網罪科偵測到超過25.5萬項與偵察活動相關的本地網絡威脅情報，佔針對香港的網絡威脅情報的17%。受偵察活動攻擊最多的三個行業分別是運輸業、醫療保健服務業和政府部門。上述數字反映攻擊者將大量資源投放於網絡攻擊鏈的前期部署階段，旨在發動實質攻擊前全面掌握目標資訊。

In 2025, CSTCB detected over 255,000 pieces of local cyber threat intelligence related to reconnaissance activities, representing 17% of the cyber threat intelligence targeting Hong Kong. The top three target industries are transportation, healthcare services and government departments. These figures reflect that attackers are allocating substantial resources to the preliminary stage of the cyber kill chain, aiming to comprehensively gather target information prior to launching an attack.


攻擊者主要透過大規模的端口掃描、軟件服務及版本檢測和作業系統檢測，系統性地探測連接互聯網的裝置，藉此識別暴露於公共網絡的伺服器或網上平台、配置失當的雲端儲存服務，以及存在已知漏洞的舊版作業系統與應用程式。根據掃描所得的情報，攻擊者可以窺探機構的網絡架構，鎖定最易入侵的弱點作為攻擊起點，從而繞過傳統防護系統。

Attackers primarily utilise large-scale port scanning, software service and version detection, and operating system detection to systematically probe public-facing devices, thereby identifying servers or web portals exposed to the public network, misconfigured cloud storage services, as well as outdated operating systems and applications with known vulnerabilities. Based on the intelligence gathered from these scans, attackers can gain insights into an institution's network architecture and pinpoint the most vulnerable entry points to serve as launchpads for attacks, bypassing traditional security systems.

## 勒索軟件與APT團伙活動
## Activities of Ransomware and APT Groups

2025年，網罪科通過網絡安全行動中心聯盟的關聯分析功能，共偵測到四個勒索軟件團伙和一個APT組織積極針對重要基礎設施發動攻擊，受攻擊的行業包括政府、航空運輸、陸路運輸、海運業、銀行及金融服務、廣播、通訊、能源、醫療保健、公共事業，以及其他重要基礎設施。透過網絡安全行動中心聯盟的情報分享、網絡安全中心的持續監控，以及重要基礎設施營運者之間的緊密合作，這些攻擊企圖均在早期階段被識別並成功遏制，從而避免了服務中斷或數據損失。

Through the threat correlation analysis of SOCA, CSTCB detected activities of four ransomware groups and one advanced persistent threat (APT) group in 2025, actively targeting critical infrastructures, including government, air transport, land transport, maritime industry, banking and financial services, broadcasting services, telecommunications, energy, healthcare services, public utilities and other key infrastructures. Leveraging intelligence sharing on SOCA, continuous monitoring by CSC, and close collaboration among critical infrastructure operators, these attack attempts were identified at an early stage and successfully contained before resulting in service disruption or data loss.


其中，LockBit仍然是全球最活躍及最具破壞力的勒索軟件集團之一，針對世界各地廣泛的關鍵行業。Superblack因利用 Fortinet防火牆的嚴重漏洞滲透高價值基礎設施及政府網絡而迅速備受關注。Warlock則利用微軟SharePoint的零日漏洞及進階持續性滲透技術，發動具嚴重影響的跨行業勒索軟件攻擊。與此同時，UNC6040專注於雲端環境，利用語音釣魚及惡意軟件即服務整合來竊取敏感機構數據。最後，Cookie Spider 結合社交工程，並透過假冒技術支援網站散播自訂惡意軟件，主要針對銀行及通訊業。

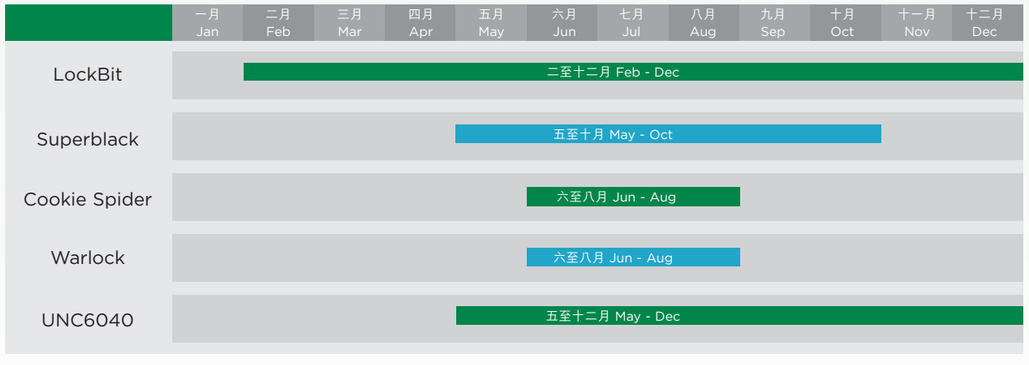
Among them, LockBit remained one of the most active and destructive ransomware groups, targeting a wide range of critical sectors worldwide. Superblack quickly gained attention for exploiting severe vulnerabilities in Fortinet firewalls to infiltrate high-value infrastructure and government networks. Warlock leveraged zero-day flaws in Microsoft SharePoint and advanced persistence techniques to deliver impactful ransomware attacks across multiple industries. Meanwhile, UNC6040 focused on cloud-based environments, using voice phishing and malicious software-as-a-service (SaaS) integrations to steal sensitive organisational data. Lastly, Cookie Spider combined social engineering with custom malware distribution through fake tech support websites, primarily targeting the banking and communications sectors.

這些團伙以利用高度客製化的釣魚與社交工程技術試圖取得初始存取權而聞名，例如攻擊者仿冒IT支援人員進行語音釣魚活動，以及建立逼真的偽造IT支援入口網站以大規模散播惡意軟件。與此同時，黑客亦嘗試利用防火牆、遠端桌面協定（RDP）端點及VPN解決方案等公開服務和應用程式的已知漏洞，試圖在Windows、Linux、ESXi和macOS等多種環境中建立立足點。

近年來，黑客團伙專注於高價值產業，採取針對性與跨行業策略，深入研究目標機構的系統並長期潛伏。多宗國際攻擊案例顯示，單一機構若要有效偵測早期威脅，必須具備完善的安全政策及偵測方案。同時，必須依靠跨機構的威脅情報共享及提升人員的安全意識，才能全面應對新型網絡威脅，確保產業安全。

The groups are known for making initial access attempts by relying on highly tailored phishing and social engineering techniques, including vishing campaigns in which attackers impersonated IT support personnel, as well as the creation of convincing fake IT support portals used to distribute malware at scale. In parallel, the hackers have attempted to exploit well-known vulnerabilities in publicly exposed services and applications, such as firewalls, Remote Desktop Protocol (RDP) endpoints, and VPN solutions, to gain footholds across multiple platforms, including Windows, Linux, ESXi, and macOS environments.

In recent years, the hacker groups have focused on high-value industries, adopting targeted and cross-sector strategies while conducting in-depth research and maintaining persistent access within the systems of target organisations. Multiple international attack cases have demonstrated that for a single organisation to detect threats early, it is essential to have robust security policies and detection solutions in place. Effective defence also depends on cross-institutional threat intelligence sharing and enhanced personnel awareness; only through these combined efforts can emerging cyber threats be comprehensively addressed and industry security ensured.




根據 2025 年數據觀察所得，各 APT 組織的活躍月份。
Timeline represents the observed active months for each APT group based on the 2025 dataset.

# 2025年網絡安全挑戰 Cybersecurity Challenges in 2025

## 人工智能驅動的網絡威脅 AI-Driven Cyber Threats

### 引言 Introduction

在 2025 年，人工智能已成為網絡安全領域的一把雙刃劍。一方面，威脅者利用生成式人工智能降低犯罪技術門檻，擴大了網絡攻擊和網上騙案的規模與逼真度；另一方面，人工智能亦為執法機構和網絡安全專業人員提供了先進的防禦工具。隨著新技術的出現，未來的人工智能軍備競賽只會加劇，這凸顯了建立強大的公私營合作夥伴關係以保障香港網絡安全環境的必要性。

In 2025, AI emerged as a double-edged sword in the realm of cybersecurity. While its advancement has lowered technical barriers for threat actors, amplifying the scale and persuasiveness of cyberattacks and online fraud, it has also equipped law enforcement agencies and cybersecurity professionals with advanced defensive tools. With the emergence of new technologies, the AI arms race will only intensify in the future, underscoring the need for robust public-private partnerships to safeguard Hong Kong's cyberspace.

### 生成式人工智能助長網上騙案 Generative AI Fuelling Online Fraud

大型語言模型能夠生成針對個別受害人、高度精細、流暢且個人化的釣魚訊息，而圖像、音頻和視頻生成工具使騙徒能夠以幾乎零成本偽造身份證明、產品圖像和宣傳材料，並建立逼真的假冒網站。在香港，2025 年涉及網上投資騙案的總損失達到 35.8 億港元，較 2024 年增加了近 60%；網上購物騙案總損失接近4億港元，增加約 10%。

LLMs can generate highly refined, fluent, and personalised messages tailored to individual victims. Meanwhile, image, audio, and video generation tools enable scammers to fabricate convincing identity proofs, product images, and promotional materials, as well as creating highly realistic fraudulent websites, at virtually no cost. In Hong Kong, losses from online investment fraud amounted to HK$3.58 billion in 2025, a nearly 60% increase from 2024, while e-shopping fraud losses approached HK$400 million, up approximately 10%.


### 人工智能在網絡攻擊中的武器化 Weaponisation of AI in Cyber Attacks

在2025年，威脅者利用了人工智能的「自主代理」特性，開發出能夠在極少人為監督下執行複雜任務的自動化系統。透過操控人工智能的編程能力，他們部署了由人工智能生成的代碼來自動化執行整個網絡攻擊鏈，從端口掃描和漏洞偵測到數據竊取，其速度與規模均前所未見，攻擊目標遍及全球的關鍵基礎設施、政府機構與企業。此外，透過「越獄」通用人工智能系統，威脅者還開發出多態惡意軟件，能在運行時動態更改代碼以逃避傳統基於特徵碼的偵測方法，並以「勒索軟件即服務」方式在暗網上銷售。

In 2025, threat actors exploited AI's "agentic" features, creating autonomous systems capable of executing complex tasks with minimal human oversight. By manipulating AI programming capabilities, they deployed AI-generated code to automate the entire chain of cyberattacks, from port scanning and vulnerability detection to data exfiltration, at unmatched speeds and scales, targeting critical infrastructures, governments, and enterprises worldwide. By jailbreaking general-purpose AI systems, they also developed polymorphic malware that dynamically alters its code at runtime to evade traditional signature-based detection, distributing it as Ransomware-as-a-Service (RaaS) on the dark web.

### 數碼信任的侵蝕 Erosion of Digital Trust

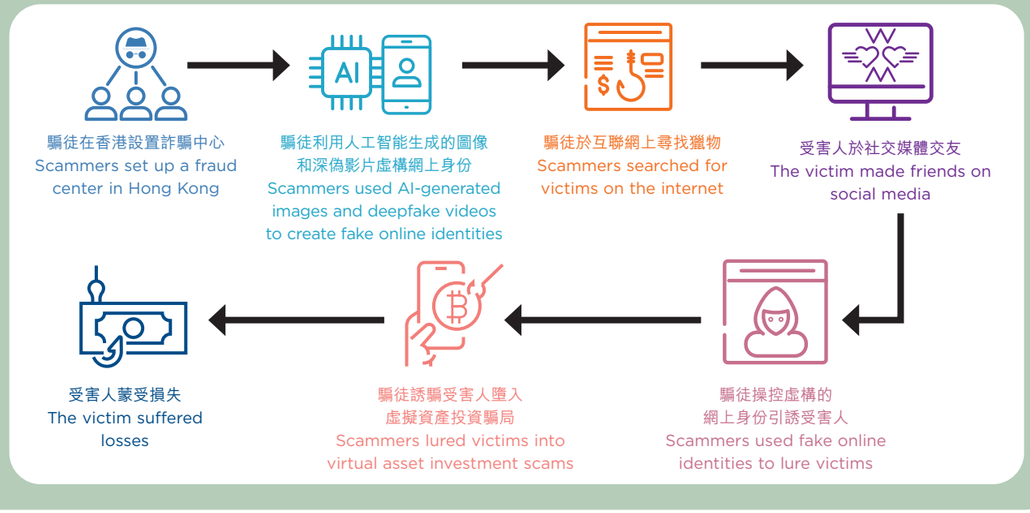
多模態深偽技術日趨成熟，能同步合成人臉、聲音與動作，生成逼真的數位人類，其水平已達「近乎無法區分」的門檻。隨著虛假資訊以這種高度逼真的形式，以前所未有的規模在社交媒體和通訊平台上傳播，公眾愈來愈難在網上區分真偽內容。在香港，2025 年有超過一半（52.2%）的受訪者表示擔心無法在網上區分真偽內容[3]。這種信任危機不僅影響個人對資訊的判斷，更可能削弱公眾對數碼金融服務、電子商務以至公共機構通訊的信心，對社會整體構成深遠影響。

Multimodal deepfake technologies have matured significantly, synchronously synthesising facial expressions, voice, and body movements to produce highly realistic digital humans that have crossed a "nearly indistinguishable" threshold. As disinformation spreads at unprecedented scale across social media and messaging platforms in such highly convincing forms, the public finds it increasingly difficult to distinguish genuine from fabricated content online. In Hong Kong, over half (52.2%) of respondents in 2025 expressed concern about distinguishing genuine from fabricated content online[3] . This trust deficit extends beyond individual information judgement—it risks undermining public confidence in digital financial services, e-commerce, and even institutional communications, with far-reaching consequences for society as a whole.

## 個案一 Case Study 1 深偽相關虛擬資產投資騙局 Deepfake-related virtual asset investment scams

2025年1月，香港警方展開代號為「暗簾」的行動，拘捕了31名涉嫌利用人工智能生成的圖像和深偽影片在社交媒體上引誘受害者墮入虛擬資產投資騙局的疑犯。該集團操控多個虛構的網上身份和兩個詐騙中心進行跨境詐騙，導致香港及其他司法管轄區的受害者蒙受逾3 400萬港元的損失。此案例反映，生成式人工智能讓騙徒能夠輕易啟用多個並行身份並與受害者進行持續且量身訂製的互動，從而使網上情緣及投資騙案趨向工業化。

In January 2025, the HKPF conducted an operation, codenamed "SECRETDRAPE", arresting 31 suspects who had used AI-generated images and deepfake videos on social media to lure victims into virtual-asset investment scams. The syndicate operated multiple synthetic online personas and two scam centres to conduct cross-border fraud, causing over HK$34 million in losses to victims in Hong Kong and other jurisdictions. This case demonstrates how generative AI facilitates the industrialisation of romance and investment scams by enabling fraudsters to operate with numerous parallel identities and maintain sustained, tailored interactions with victims.

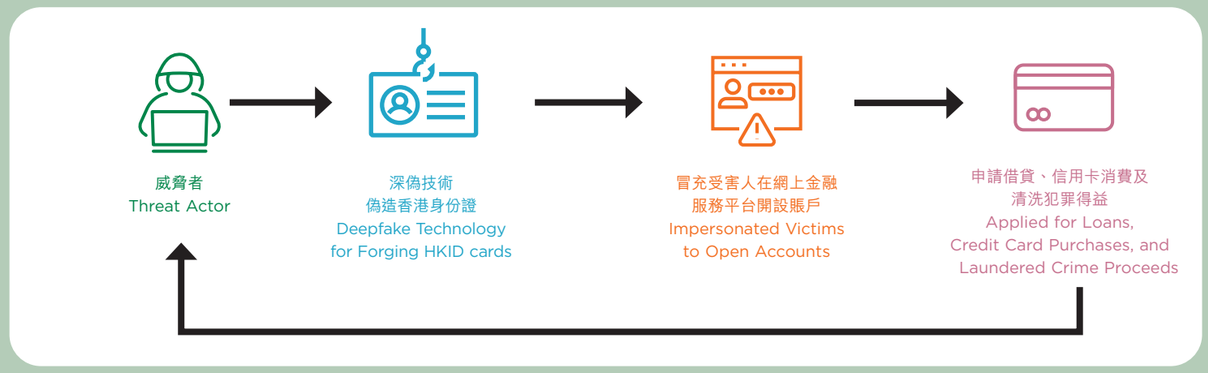



[3] P.33, Reuters Institute Digital News Report (Hong Kong) 2025. School of Journalism and Communication, The Chinese University of Hong Kong. https://ccpos.com.cuhk.edu.hk/ReportHK2025.pdf

## 個案二 Case Study 2 人工智能驅動的虛假身份 AI-powered fake identity

2025年，香港警方瓦解了兩個利用人工智能深偽技術偽造身份的犯案集團，合共拘捕20名疑犯。2025年4月，警方在代號「智鬥」的行動中拘捕9名疑犯，調查揭發集團利用深偽技術將成員的五官融入已報失身份證的頭像中，再上載自拍影像冒充持證人，其後利用所開設的戶口申請借貸、進行信用卡消費及清洗約120萬港元犯罪得益。2025年12月，警方再揭發另一集團利用深偽技術偽造香港身份證並拘捕11名疑犯，該集團涉嫌冒充受害人，透過數碼身份認證程序在網上金融服務平台開設賬戶，繼而盜取受害人的資產。這些案件反映，騙徒正濫用人工智能技術擴大犯罪活動規模，並將攻擊目標由個人轉向金融機構及網上金融服務平台的身份驗證機制，此舉對數碼身份驗證體系的可信度構成挑戰。

In 2025, the HKPF neutralised two criminal syndicates that had exploited AI deepfake technology to forge identities, resulting in the arrest of 20 suspects. In April 2025, police arrested nine suspects in Operation WITSGAME and uncovered a syndicate that had used deepfake technology to merge members' facial features into the photos on reported-lost identity cards and had uploaded selfie footage to impersonate the cardholders. The fraudulently opened accounts were subsequently used to apply for loans, make credit card purchases, and launder criminal proceeds amounting to HK$1.2 million. In December 2025, police uncovered another syndicate and arrested 11 suspects who had used deepfake technology to forge Hong Kong identity cards, impersonating victims to open accounts on online financial services platforms through digital identity verification procedures and subsequently stealing their assets. These cases underscore how fraudsters are misusing AI technologies to scale criminal operations, shifting their targets from individuals to the identity verification mechanisms of financial institutions and online financial services platforms, thereby challenging the credibility of digital identity verification systems.




## 卡巴斯基 kaspersky 對抗 AI 自動化網絡攻擊 Kaspersky: Combating AI-automated cyberattacks

卡巴斯基觀察到威脅者正日益廣泛地採用人工智能系統，例如大型語言模型和多模態模型。在調查各類網絡攻擊的過程中，卡巴斯基發現了威脅者在籌備及發動攻擊時應用人工智能的多種手法。

儘管通常難以斷定某段文字是否絕對由大型語言模型生成，但仍有一些跡象能提供高度的可信度。舉例來說，惡意程式碼中若出現過多、甚至是不必要的表情符號和註釋，往往是人工智能生成代碼的典型特徵，卡巴斯基便在 BlueNoroff APT[4] 組織所使用的竊密模組中識別出了這類痕跡。另一例子則是技術邏輯上的不一致，例如過多的匯入以及宣告了卻未使用的函數——這類異常現象曾出現在勒索軟件組織 FunkSec[5] 的代碼中。而在針對加密貨幣用戶的自動化釣魚攻擊[6]中，還發現了另一種痕跡：即包含大型語言模型的「拒絕回應」內容。此外，威脅者有時會在攻擊活動中使用合成媒體（如圖像），這可從元數據中看出端倪：前述的 BlueNoroff APT 就曾利用從社交網絡收集、並經由多模態大型語言模型編輯過的圖像，因而留下了相應的EXIF痕跡。

雖然威脅者顯然正積極利用人工智能，但預計這並不會徹底改變網絡安全的整體格局。儘管大型語言模型提升了攻擊者的能力並助其擴大行動規模，但其核心戰術與技術並未改變。然而，隨著網絡攻擊數量增加且節奏加快，可能會令網絡安全專業人員疲於奔命，特別是在人手本已短缺的情況下。這凸顯了業界對於更先進的網絡安全中心自動化，以及在網絡安全解決方案中更廣泛採用人工智能技術的迫切需求。

Kaspersky is seeing growing adoption of AI systems, such as LLMs and multimodal models, among threat actors. While investigating various cyberattacks, Kaspersky has stumbled upon different applications of AI by threat actors when preparing for and launching cyberattacks.

While there is usually no way to definitively prove that a piece of text was created with the help of an LLM, there are some telltale signs which can give us a high level of certainty. For example, excessive use of emojis and comments (sometimes unnecessary) in malicious scripts is a typical indicator of AI-generated code. Kaspersky has identified such artefacts in a stealer module used by a BlueNoroff APT[4] . Another example is technical inconsistencies, such as excessive imports and declared but unused functions—an anomaly observed in the code used by the ransomware group FunkSec[5] . Other artefacts found in automated phishing attacks[6] against cryptocurrency users are LLM refusals. Moreover, threat actors sometimes use synthetic media, such as images, in their campaigns, which can be evident from image metadata: the aforementioned BlueNoroff APT used images harvested from social networks and edited with a multimodal LLM, leaving respective EXIF traces.

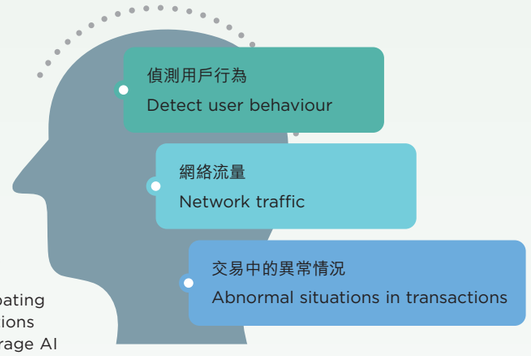
While it is evident that threat actors are very active in their use of AI, the cybersecurity landscape is not expected to be radically reshaped. While LLMs provide a capability uplift and help to scale their operations, the tactics and techniques remain the same. However, the growing number of cyberattacks and their increasing pace may strain cybersecurity professionals, especially when they are already understaffed. This underlines the growing need for more advanced SOC automation and wider adoption of AI technologies in cybersecurity solutions.

[4] Ryu, S., & Amin, O. (2025, October 28). Crypto wasted: BlueNoroff's ghost mirage of funding and jobs. Securelist by Kaspersky. https://securelist.com/bluenoroffapt-campaigns-ghostcall-and-ghosthire/117842/
[5] Kaspersky. (2025, July 3). Inside FunkSec: Kaspersky explores the evolution of AI-powered ransomware with password-gated capabilities. https://meen.kaspersky.com/about/press-releases/kaspersky-explores-the-evolution-of-ai-powered-ransomware-with-password-gated-capabilities
[6] Tushkanov, V. (2024, October 31). Loose-lipped neural networks and lazy scammers. Securelist by Kaspersky. https://securelist.com/llm-phish-blunders/114367/

## 人工智能的防禦性應用 Defensive Applications of AI

人工智能驅動的防禦已被視為現代網絡安全策略中不可或缺的一環。網絡安全專業人員正加速部署人工智能，以偵測用戶行為、網絡流量和交易中的異常情況，主要應用範疇包括網絡釣魚偵測、入侵事件應變及用戶行為分析等。在打擊網上騙案方面，電訊供應商和平台利用人工智能進行全天候監控，學習正常行為模式並實時標記可疑活動，在受害者蒙受損失前攔截可疑交易；智能手機和通訊應用程式亦整合裝置端人工智能以識別詐騙指標，社交網絡和廣告平台則透過人工智能內容過濾器偵測詐騙網址和深偽內容。

AI-powered defence is increasingly seen as an indispensable component of modern cybersecurity strategies. Cybersecurity professionals are expediting AI deployment to detect anomalies in user behaviour, network traffic and transactions, with primary applications including phishing detection, intrusion response and user-behaviour analytics. In combating online fraud, telecommunications providers and platforms leverage AI for round-the-clock monitoring that learns normal behavioural patterns and flags suspicious activities in real time, blocking fraudulent transactions before victims incur losses; smartphones and messaging apps also integrate on-device AI to identify scam indicators, while social networks and advertising platforms employ AI content filters to detect scam URLs and deepfake content.




2025 年，香港警務處推出了「RAPID 引擎」，部署人工智能以分析可疑網站。利用人工智能算法，RAPID 引擎根據域名特徵、可疑代碼和品牌標誌識別等多維度規則進行實時分析。威脅情報會同步更新至「防騙視伏器」系列，並分發予多個互聯網服務供應商進行攔截，從而有效提升公眾防範網絡釣魚威脅和網上騙案的能力。

In 2025, the HKPF launched the RAPID Engine, which deploys AI to analyse suspicious websites. Utilising AI algorithms, the RAPID Engine performs real-time analysis based on multidimensional rules such as domain characteristics, suspicious codes and the recognition of brand logos. Threat intelligence is simultaneously updated to the "Scameter Series" and disseminated to multiple internet service providers for blocking, effectively strengthening public protection against phishing threats and online frauds.

## 雲端安全的挑戰 Cloud Security Challenges

### 引言 Introduction

在 2025 年，雲端安全風險仍然顯著。由於大量關鍵業務功能透過雲端服務供應商運作，並採用「共同責任模式」，即客戶與供應商各自承擔明確的安全責任，因此風險管理更為複雜。香港網絡安全事故協調中心（HKCERT）亦指出雲端平台已成為企業日常營運的基礎設施，並將「過度依賴單一雲端基礎設施導致營運中斷風險」列為其2026年五大網絡安全風險之一[7]。

Cloud security risk remained significant in 2025, as numerous business-critical functions were operated through cloud service providers under a shared responsibility model, where both the customers and the providers had defined security obligations. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) also highlighted that cloud platforms had become the backbone of enterprise operations and identified "Over-Reliance on Cloud Infrastructure Creates Single Points of Failure" as one of the top five cybersecurity risks in 2026[7].

### 個案三 Case Study 3 — 針對香港證券公司的網絡入侵事件 Cyber intrusion against a Hong Kong based securities firm

2025年5月至6月期間，一間提供加密貨幣相關交易服務的香港證券公司遭受多階段網絡入侵，涉及多個雲端與本地環境。此事件清楚展示了當配置漏洞、憑證濫用及可視性不足三者結合時所帶來的嚴重風險。

攻擊始於部署在雲端「用戶驗收測試」(UAT)環境中的一項過時排程系統元件。由於身份驗證控管不足，攻擊者得以注入惡意程式碼以建立初步立足點，並部署客製化後門程式與外部命令與控制伺服器進行通訊，同時刪除日誌以妨礙鑑證分析。

攻擊者其後透過已遭入侵的VPN設備進行橫向移動，利用過時韌體及未停用的閒置帳戶逐步擴大入侵範圍。其後，攻擊者使用高權限的預設管理帳戶存取生產環境資料庫，濫用允許執行作業系統命令的合法資料庫功能，並停用該功能以規避偵測。攻擊者亦在多個環境中部署入侵後工具組，從記憶體竊取憑證，並採用模仿合法系統命令的隱藏技術維持長期存取。

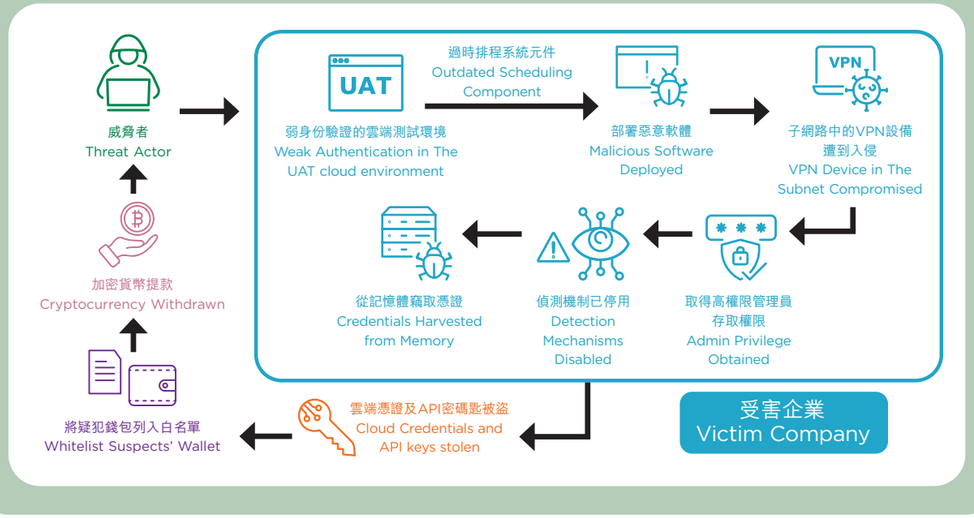
攻擊最終以竊取資金收場。攻擊者利用被竊取的雲端憑證存取第三方平台API密碼匙，將外部錢包列入白名單並執行加密貨幣提款。

Between May and June 2025, a Hong Kong securities firm operating cryptocurrency-related trading services was targeted in a multi-stage cyber intrusion that affected cloud and on-premises environments. This incident illustrates the compounded risk that arises when configuration vulnerabilities, credential abuse, and visibility gaps converge.

The attack originated from an outdated scheduling component in a cloud-hosted User-Acceptance Test (UAT) environment. Insufficient authentication controls enabled the attacker to inject malicious code, establish a foothold, and deploy a custom backdoor communicating with an external command-and-control (C2) server, while deleting logs to hinder forensic analysis.

The attacker then moved laterally through a compromised VPN device, exploiting outdated firmware and idle accounts that had not been disabled to progressively expand the intrusion. Subsequently, using a high-privilege default administrative account, the attacker authenticated to a production database and abused legitimate database features to execute system commands, later disabling those features afterward to avoid detection. The attacker also deployed post-exploitation toolkits across multiple environments to harvest credentials from memory and maintained persistence using process-hiding techniques mimicking legitimate system commands.

The attack culminated in financial theft. Compromised cloud credentials were used to access third-party platform API keys, whitelist external wallets, and execute cryptocurrency withdrawals.




[7] HKCERT. (2026, January 29). Hong Kong Cybersecurity Outlook 2026: Security incidents hit record high with 27% annual increase. https://www.hkcert.org/press-centre/hkcert-releases-hong-kong-cybersecurity-outlook-2026-security-incidents-hit-record-high-with-27-annual-increase-ai-related-attacks-and-supply-chain-risks-emerge-as-top-concerns-nearly-30-of-enterprises-lack-dedicated-cybersecurity-personnel

### 雲端配置漏洞 Cloud Configuration Vulnerabilities

雲端配置的常見弱點包括儲存空間意外暴露、過於寬鬆的網絡規則及存取控制設定錯誤。造成雲端資料外洩的常見原因並非「黑客入侵」，而是意外暴露。一旦權限被錯誤設定，儲存空間可能變為公開可讀取，任何人只要取得連結即可存取資料。在香港受監管的環境中，單一雲端元件的暴露便可能導致個人資料外洩，進而引發監管審查及聲譽損害。攻擊者通常採取自動化方式搜尋被暴露的端點及配置錯誤的資源，繼而濫用憑證或利用防護不足的管理介面以擴大存取範圍。

Common weaknesses in cloud configuration include unintended public exposure of storage, permissive network rules, and misconfigured access controls. A prevalent cause of cloud data leaks is not hacking but accidental exposure. When permissions are misconfigured, storage can become publicly readable to anyone with the link. In Hong Kong's regulated environment, a single exposed cloud component can lead to a personal data breach and trigger regulatory scrutiny and reputational damage. Attackers routinely use automated discovery of exposed endpoints and misconfigured resources, followed by credential abuse or exploitation of weakly protected administrative interfaces to expand access.

### 欠缺雲端可視性 Lack of Cloud Visibility

許多機構在不同帳戶、專案及地區之間，對雲端控制平面的日誌記錄覆蓋並不完整，從而削弱了威脅偵測及事後鑑證分析能力。部分機構對閒置帳戶缺乏管理或未納入日誌覆蓋範圍，造成可視性缺口。一旦帳戶遭入侵，攻擊者可能利用未監控的區域進行橫向移動或權限提升。日誌管理應涵蓋生成、傳輸、儲存、存取及銷毀等生命周期流程，並明確涵蓋雲端環境，從而為所有系統建立端到端的日誌治理。

Many organisations have incomplete control plane logging coverage across accounts, projects, and regions, which weakens detection and forensic reconstruction. Idle accounts that are unmanaged or excluded from logging coverage create visibility gaps. Once compromised, attackers may exploit these unmonitored areas to facilitate lateral movement or privilege escalation. Log management should span the full lifecycle, including generation, transmission, storage, access, and disposal, and explicitly cover cloud environments to establish end-to-end logging governance.

### 憑證、權標及API密碼匙濫用 Credential, Token, and API key Abuse

雲端入侵事件往往與身份識別息息相關。缺乏存取控制或使用弱密碼會令攻擊者容易利用憑證填充或暴力破解手法，入侵合法的雲端API及管理流程以操作系統，而無需部署容易被偵測的惡意程式。攻擊者常見的持續性存取手法包括在雲端帳戶或服務主體中加入由攻擊者控制的憑證，並利用常見的雲端服務將數據竊取混入日常流量中，以降低偵測風險。

Cloud compromises frequently pivot on identity. The lack of access controls or the use of weak passwords can enable attackers to intrude into legitimate cloud APIs and administrative workflows to manipulate systems without deploying detectable malware. Attackers' common persistence methods include adding attacker-controlled credentials to cloud accounts or service principals, while leveraging common cloud services to conceal data exfiltration with normal traffic and evade detection.

### 阿里雲 Alibaba Cloud

全球雲與人工智能安全態勢呈現「攻防加速、風險交織」的新特徵。
Alibaba Cloud: Global Cloud and AI Security Posture Shows New Characteristics of Accelerated Offense-Defence Dynamics and Intertwined Risks.

據阿里雲安全態勢監測數據顯示，2025年12月雲平台日均防禦攻擊達72.28億次，按月上升7.65%，雲上攻擊持續處於高位運行，雲平台已實現極高水位的預設防禦能力。同時，88%的企業正透過雲原生技術實現自動化防禦，利用雲端原生安全機制應對高頻攻擊。

人工智能技術的雙刃劍效應日益凸顯。一方面，2025年人工智能代理應用的激增帶來了新型攻擊面，大模型越獄、提示詞注入等風險成為全球安全焦點；利用大模型生成的深度偽造內容亦呈爆發式增長。在雲端場景中，攻擊者可利用深偽身份或語音進行帳戶接管，間接導致雲端入侵。另一方面，人工智能驅動的威脅偵測與自動化回應將成為2026年的核心防禦能力，能將威脅回應速度由小時級大幅提升至秒級。

According to Alibaba Cloud security posture monitoring data, cloud platforms defended against an average of 7.228 billion attacks per day in December 2025, reflecting a 7.65% month-on-month increase. Cloud-borne attacks remain at persistently high levels, while cloud platforms have achieved an exceptionally robust default defence posture. Meanwhile, 88% of enterprises have adopted cloud-native technologies to enable automated defence, leveraging built-in cloud security capabilities to effectively counter high-frequency attacks.

The dual nature of AI technologies is becoming increasingly evident. On one hand, the rapid proliferation of AI Agent applications in 2025 has expanded the attack surface, with risks such as large language model jailbreaking and prompt injection emerging as major global security concerns. Deepfakes generated by large models have also experienced explosive growth. In cloud environments, attackers can leverage deepfake identities or voice simulations to execute account takeovers, indirectly leading to cloud compromises. On the other hand, AI-powered threat detection and automated response are set to become core defensive capabilities in 2026, shortening threat response times from hours to seconds.

## 供應鏈及第三方漏洞 Supply Chain and Third-Party Vulnerabilities

### 引言 Introduction

供應鏈攻擊是一種影響深遠的初始入侵途徑。攻擊者可濫用受信任的開發、分發及更新渠道，而無須直接突破目標機構的邊界防護。在香港，不少機構高度依賴第三方資訊科技方案及外判服務，令此類風險在營運層面尤為突出。一旦供應商端出現失誤，例如更新前測試不足、自動更新欠缺用戶端管控，或第三方軟件風險管理鬆散，其影響可迅速蔓延至大量下游機構。

Supply chain compromise is a high-impact initial access vector. Attackers can abuse trusted development, distribution, and update channels, rather than directly breaching a target's perimeter. In Hong Kong, the risk is particularly significant at the operational level as many organisations depend heavily on third-party IT solutions and outsourcing. A single provider-side failure can cascade downstream, driven by inadequate pre-release testing, uncontrolled automatic updates, and weak third-party software risk management.

### 開發流程及依賴鏈受損
### Compromised Development Pipelines and Dependency Abuse

攻擊者針對開發工具及管道，將惡意程式碼植入合法軟件產物。其中一種常見手法包括濫用依賴鏈。由於不少建置環境對公開套件庫的信任設定過於寬鬆，或缺乏嚴格的依賴解析控制，惡意套件得以在建置過程中被自動擷取並執行。當企業自動部署供應商更新時，可能導致大規模下游暴露，使惡意程式迅速傳播至生產環境，波及面向客戶及受監管的服務。開源依賴項進一步加劇此問題，因為許多機構對自身軟件所包含的元件及其實際應用範圍缺乏全面掌握，一旦依賴項出現問題，往往難以及時採取遏制措施或確定修補優先次序。

Attackers target development tools and pipelines to insert malicious code into legitimate software artefacts. A common path is dependency chain abuse, where build environments fetch and execute malicious packages due to weak dependency resolution controls or default trust in public registries. This can lead to large-scale downstream exposure when enterprises auto-deploy vendor updates, resulting in rapid propagation into production environments and potential disruption of customer-facing and regulated services. Open-source dependencies amplify this risk. Many organisations lack full visibility of what components are embedded in their software, delaying containment and patch prioritisation when a dependency is compromised.

### 個案四 Case Study 4　透過外判數碼身份認證及第三方開戶流程進行的身份詐騙
### Identity fraud via outsourced digital identity verification and third-party onboarding pathway

2025年，網罪科接獲一宗來自公營機構的通報，指有騙徒涉嫌使用偽造身份證冒充受害人，開設網上會員帳戶並從該機構的平台盜取資產。涉事平台採用多供應商模式開發，總承辦商將數碼身份驗證及開戶等核心功能，分判予不同專業供應商負責。

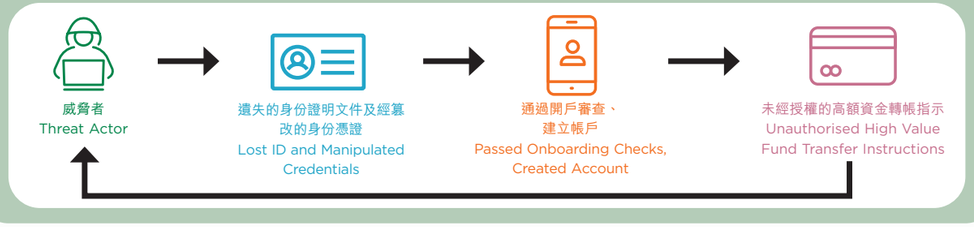
In 2025, CSTCB received a report from a public sector organisation about fraudsters suspected of using forged identity cards to impersonate victims, creating online member accounts and stealing assets from the organisation's platform. The platform was built under a multi-vendor supply chain model, with the prime contractor engaging specialist subcontractors for digital identity verification and customer onboarding.

本案的入侵方式並非利用軟件漏洞，而是濫用多方共享責任機制及端對端管控之間的缺口。騙徒憑藉一份遺失的身份證明文件及經篡改的身份憑證，成功通過開戶審查、建立帳戶，並提交未經授權的高額資金轉帳指示。從供應鏈角度審視，本案暴露出三個關鍵問題。其一，身份認證職能分散於平台營運者、總承辦商、數碼身份認證服務供應商及下游金融機構等多方之間，沒有任何一方能全面掌握端對端的風險。其二，開戶流程容許透過文件掃描及遙距驗證完成註冊，騙徒藉此途徑在系統中建立了一個表面「合法」的數碼身份。其三，攻擊者能同時經網上渠道及實體服務中心進行敏感的帳戶變更操作，反映不同渠道之間的驗證標準存在差異，對關鍵操作亦欠缺有效的強化驗證機制。

Rather than exploiting software vulnerabilities, the attacker abused gaps in shared responsibilities and end-to-end controls. Using a lost identity document and manipulated credentials, the fraudster passed onboarding checks, created an account, and submitted unauthorised high-value fund transfer instructions. Three supply chain dimensions were critical. First, identity verification was fragmented across the platform operator, prime contractor, digital identity verification service vendor, and downstream financial service providers, meaning no single party owned the end-to-end risk. Second, the onboarding pathway permitted account creation via document scanning and remote verification, which the fraudster exploited to establish a seemingly legitimate digital identity. Third, inconsistent verification standards across online and physical channels created gaps that allowed sensitive account changes without adequate step-up authentication.

此事件造成重大財務損失，同時損害了機構的公眾信譽，並需要緊急檢討及重整內部控制。本案清楚說明，在由供應鏈交付的平台環境中，最大的風險往往並非軟件層面的技術漏洞，而是流程設計及各方保證機制上的不足。

The incident caused significant financial loss along with reputational damage and required urgent control redesign. It demonstrates that on platforms delivered through supply chains, the primary risk often lies in process integrity and assurance gaps, not only software security.




### 以身份為核心的軟件即服務平台攻擊
### Identity-Driven SaaS platform compromises

許多軟件即服務（SaaS）入侵事件以身份為核心。攻擊者常用的手段之一是「同意網絡釣魚」，即透過誘使用戶向惡意應用程式授予OAuth權限，在無需於端點安裝惡意程式的情況下，直接存取電子郵件、檔案及協作數據。由於SaaS平台往往深度融入企業的日常業務流程，一旦遭入侵，可直接引發商業電郵詐騙、發票騙案及數據外洩，並透過客戶關係管理系統、工單系統及財務自動化等整合介面進一步擴散。此外，部分機構在採用第三方平台時，並未核實供應商是否在系統底層保存完整的操作日誌，導致發生事故後難以迅速取得相關紀錄，嚴重妨礙調查及舉證工作。

Many SaaS compromises are identity-driven. Attackers use valid accounts or abuse accounts' access in cloud and SaaS environments to achieve access, persistence, and privilege escalation. Through consent phishing, attackers trick users into granting malicious applications OAuth permissions, enabling access to email, files, and collaboration data without deploying endpoint malware. Because SaaS platforms are deeply integrated into business workflows, such compromises can directly enable business email compromise, invoice fraud, data leakage, and lateral movement through customer relationship management (CRM), ticketing, and finance automation integrations. Some organisations also fail to verify whether third-party platforms retain system-level operation logs, which can severely hinder incident investigation and evidence submission.

### 不受控的第三方存取及遠端管理
### Uncontrolled Third-Party Access and Remote Management

第三方通常需要具有特權的連接方式，包括支援帳戶、遠端管理工具及API存取權限，這擴大了受信任的存取面。倘若第三方的安全控制措施未及客戶的標準，這些連接便可能成為橫向移動的跳板。在多供應商協作的交付模式下，身份驗證及安全責任分散於不同持份者之間，容易出現管控真空，以致沒有任何一方能全面掌握端對端的風險全貌，也欠缺明確的問責機制。

Third parties often require privileged connectivity, including support accounts, remote management tooling and API access, which expands the trusted access surface. If a third party's security controls fall below the customer's standards, these connections become springboards for lateral movement. In multi-vendor delivery models, identity verification and security responsibilities become fragmented across parties, creating gaps where no single entity has full visibility or accountability for end-to-end risk.

深信服科技 SANGFOR

### 供應鏈攻擊的新途徑與漏洞
### Sangfor: New supply chain attack vectors & vulnerabilities

當前的網絡安全威脅形勢顯示，攻擊者正從直接入侵軟件轉向更隱蔽地濫用企業對數碼供應鏈的信任，藉此繞過傳統安全防線。

The current threat landscape shows adversaries shifting from direct software breaches to exploiting the trust organisations place in their digital supply chains, effectively bypassing traditional security perimeters.

2025 年 9 月，一隻代號「Shai-Hulud」的惡意蠕蟲利用全球最大的開源軟體共享平台「npm」的權限漏洞，在 72 小時內引發全球性連鎖感染。攻擊者透過社交工程劫持了擁有數十億下載量的核心套件維護者帳號。工程師一旦按照慣常流程下載並安裝，受污染版本的惡意代碼便會掃描電腦上儲存的平台登入憑證，從而盜用開發者身份。隨後，蠕蟲自動掃描受害者名下所有專案，將惡意代碼植入專案中，使惡意軟體隨合法更新一併分發給下游使用者。這種指數級的裂變式傳播將單點污染演變為數碼瘟疫，其最終目的並非單純竊取資料，而是令全球開發生態陷入全面癱瘓。

In September 2025, a worm codenamed "Shai-Hulud" exploited vulnerabilities in the world's largest open-source software sharing platform "npm" to achieve global chain infection within 72 hours. Attackers used social engineering to hijack maintainer accounts behind cornerstone packages with billions of downloads. Once an engineer followed the routine process of downloading and installing a contaminated version, a malicious script scanned the locally stored platform login credentials and seized the developer's identity. The worm then automatically injected malicious code into all the victim's projects, ensuring downstream distribution via legitimate updates. This exponential, fission-like spread transformed single-point contamination into a digital plague — the endgame being total operational paralysis, not mere data theft.

為緩解此類風險，企業須採取主動策略：對所有外部依賴項貫徹零信任原則，實施嚴格的依賴項掃描與軟件物料清單（SBOM）追蹤，確保構建環境相互隔離，並透過安全憑證管理系統嚴控關鍵權標。

To mitigate these risks, organisations must adopt proactive strategies: apply Zero Trust to all external dependencies, implement rigorous dependency scanning with Software Bill of Materials (SBOM) tracking, isolate build environments, and manage critical tokens through secure credential management systems.

然而，隨著攻擊者利用人工智能生成逼真的社交工程攻勢並加速橫向移動，靜態防禦已不足夠。現代防禦必須整合人工智能驅動的行為分析，利用機器學習建立正常行為基準，以便在惡意依賴注入的萌芽階段即加以偵測。人工智能驅動的自動化事件應變更能在毫秒間隔離受入侵環境、封鎖可疑套件，搶在攻擊蔓延前予以阻斷。

As attackers integrate AI to craft hyper-realistic social engineering and accelerate lateral movement, static defences are no longer sufficient. Modern defence must incorporate AI-driven behavioural analytics, using machine learning to baseline normal activity and detect malicious dependency injection at its earliest stage. AI-powered automated incident response can then isolate compromised environments and quarantine suspicious packages within milliseconds — outpacing attackers before propagation takes hold.

## 物聯網安全風險 IoT Security Risks

### 引言 Introduction

2025年，香港持續推進智慧城市發展及創新科技應用，推動物聯網技術於各行業及家庭廣泛採用。隨着路由器、網絡攝影機及智能機械人等聯網裝置的使用量不斷增加，潛在的攻擊面亦隨之擴大，物聯網已成為城市運作及數碼轉型的核心支柱。然而，許多裝置在部署時仍沿用預設的弱保安設定，一旦遭入侵，往往被改造成為代理節點、偵察工具、橫向移動跳板，甚至成為殭屍網絡或分散式阻斷服務攻擊等大規模攻擊的一部分。香港寬頻覆蓋率高、裝置更替頻繁，加上消費級遠端存取功能的廣泛使用，令相關風險更為突出。

In 2025, Hong Kong continued to advance its smart city agenda and foster innovation, driving widespread adoption of Internet of Things (IoT) technologies across industries and households. As reliance on connected devices such as routers, IP cameras, and smart robotic systems grew, so did the attack surface, making IoT a core pillar of urban operations and digital transformation. Many devices are still deployed with weak default settings and, once compromised, they can be repurposed as proxy nodes, reconnaissance tools, lateral movement pivots, or components of large-scale attack infrastructure like botnets and DDoS campaigns. Hong Kong's dense broadband coverage, frequent device turnover, and widespread use of consumer-grade remote access features make the city particularly exposed to these risks.

### 網絡攝影機被入侵 Compromised IP Cameras

攻擊者透過多種途徑入侵網絡攝影機，包括預設或重複使用的密碼、暴露於互聯網的管理介面、RTSP及ONVIF等舊式通訊協定、韌體更新不足，以及供應商雲端帳戶被盜用。取得存取權限後，攻擊者可窺看即時影像、橫向滲透至內部網絡，或將攝影機編入殭屍網絡。此類入侵不僅造成住宅、商舖和大廈公共空間的私隱外洩，亦損害企業聲譽。若攝影機與銷售點(POS)系統、網絡儲存設備(NAS)或辦公電腦處於同一網絡而未作分段隔離，更可成為攻擊者深入滲透企業內部的跳板。

Attackers target IP cameras through multiple vectors: default or reused passwords, internet-exposed administration panels, legacy protocols such as RTSP and ONVIF, inadequate firmware patching, and vendor cloud account takeovers. Once access is obtained, attackers can view live video feeds, pivot laterally into local networks, or recruit cameras into botnets. Compromise leads to serious privacy exposure affecting homes, shops, and building common areas, alongside reputational damage for businesses. Where cameras share flat networks with point-of-sale (POS) systems, network attached storage (NAS), or workstations, they can also serve as a foothold for deeper intrusions into the organisation.

### 路由器遭攻陷作為代理伺服器 Compromised Routers As Proxy Servers

攻擊者透過自動化大規模互聯網掃描，尋找存在漏洞的路由器，並利用已知弱點及預設或薄弱的登入憑證入侵裝置。取得控制權後，攻擊者會在非標準連接埠部署輕量級安全外殼協議(SSH)等後門服務，並修改路由設定以建立持久的流量中轉能力。受入侵路由器隨即成為「乾淨」的住宅或中小企出口節點，讓攻擊者藉此隱匿身份，從事憑證填充、入侵嘗試及網絡詐騙等活動，大幅增加追溯來源及跨境調查的難度。即使受入侵的路由器數目不多，亦足以組成一個具規模的代理節點池，其流量能混入正常的住宅IP位址範圍之中，極具隱蔽性。

Attackers conducted automated internet-wide scanning to identify vulnerable routers, exploiting known vulnerabilities and weak or default credentials to gain access. Once compromised, they would deploy backdoor services such as lightweight Secure Shell Protocol (SSH) on non-standard ports and modify routing configurations to establish persistent traffic relay capabilities. The compromised routers effectively become "clean" residential or SME exit nodes, allowing attackers to anonymise activities such as credential stuffing, intrusion attempts, and fraud. This makes attribution significantly harder and increases cross-border investigative workload. Even a small number of compromised routers can form a substantial proxy pool whose traffic blends seamlessly into normal household IP ranges.

### 智能裝置或機械人被劫持 Hijacked Smart Devices or Robots

隨着智能裝置及機械人在物流、零售和設施管理等領域加速普及，攻擊者正利用遠端管理介面、欠缺保護的API、過時的嵌入式作業系統，以及智能子系統與核心業務網絡之間分段不足等弱點發動攻擊。一旦成功入侵，可導致營運中斷、引發人身安全隱患，甚至洩露遙測數據、影像及環境地圖等敏感資料。隨着商業環境中的部署規模日增，這類威脅已從理論層面演變為切實的營運風險，機構必須透過妥善的網絡隔離及裝置生命周期管理加以應對。

As smart device and robotic adoption accelerate in logistics, retail, and facilities management, attackers are exploiting remote management interfaces, unsecured APIs, outdated embedded operating systems, and insufficient segmentation between smart subsystems and core business networks. Successful compromise can disrupt operations, create physical safety hazards, and leak sensitive data including telemetry, video footage, and environment mapping data. With growing deployment across commercial settings, this threat has moved beyond theoretical concern to become a tangible operational risk that organisations must address through proper network isolation and device lifecycle management.

### 個案五 Case Study 5 — 路由器遭攻陷並用作代理基礎設施 Router compromises used as proxy infrastructure

2025 年 6 月，網罪科發現有網絡罪犯透過攻陷家用路由器並將其轉用作代理節點，以協助進行針對性的網絡攻擊。後續分析確認有217 個香港IP地址遭濫用作代理節點，而這些IP地址主要是家居寬頻連線，亦包含小部分中小企網絡(如咖啡店)。

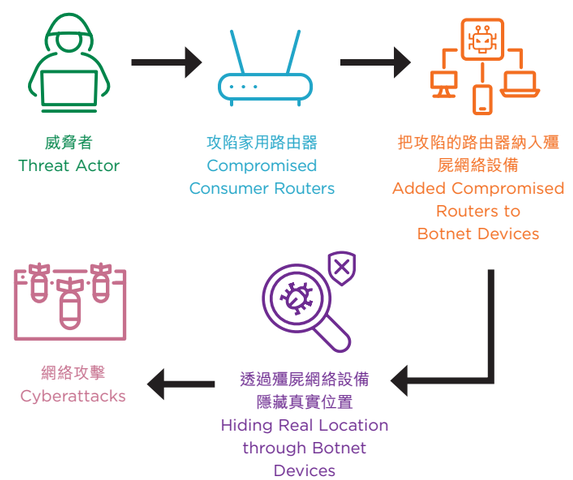
In June 2025, CSTCB identified that cybercriminals had compromised consumer routers and were repurposing them as proxy nodes to facilitate targeted cyberattacks. Follow-up analysis confirmed that 217 Hong Kong IP addresses were abused as proxy nodes, predominantly household broadband connections along with a small number of SME networks such as coffee shops.

調查顯示，是次攻擊屬於針對暴露於互聯網路由器的自動化大規模入侵。分析期間觀察到的一個關鍵感染指標，是 Dropbear SSH服務在異常高位連接埠上被啟用，顯示攻擊者已建立遠端存取權限。為維持持久控制，攻擊者在非標準連接埠部署輕量級SSH服務。受入侵的路由器隨後被設定為透過隧道或類似VPN的路由方式中轉流量，將消費者及中小企的互聯網連線轉化為「乾淨」的出口節點，最終被編入更大規模的殭屍網絡及代理基礎設施，為針對外部目標的入侵行動提供支援。

Investigation revealed that the attack was part of automated large-scale exploitation of Internet-exposed routers. A key infection indicator observed during analysis was the presence of Dropbear SSH service enabled on an unusual high port, suggesting attacker-established remote access. The compromised routers were then configured to relay traffic through tunnelling or VPN-like routing, converting consumer and SME internet connections into "clean" exit nodes. These devices were ultimately incorporated into a broader botnet and proxy infrastructure supporting intrusion attempts against external targets.

網罪科利用開源情報偵測技術及內部分析鎖定217個受影響 IP 位址，並將相關情報納入「淨網行動」框架，同時聯同相關互聯網服務供應商通知受影響客戶，提供針對性的保安指引以加快修復進度。此事件反映消費級物聯網裝置可被迅速轉化為高價值的攻擊基礎設施，同時凸顯了邊緣裝置安全配置及適時修補更新、防止管理介面暴露於互聯網，以及透過互聯網服務供應商迅速通知客戶以縮短受入侵節點存活時間的重要性。

CSTCB used OSINT-driven discovery and internal analysis to identify the 217 affected IPs and integrated the intelligence into its "Cyber Hygiene Operation" framework. Coordinated remediation was carried out with relevant ISPs to notify affected customers and provide targeted security guidance. This incident illustrates how consumer-grade IoT devices can be rapidly converted into high-value attack infrastructure. It also reinforces the importance of secure configuration and timely patching for edge devices, preventing internet exposure of management interfaces, and rapid ISP-enabled customer notification to reduce the operational lifetime of compromised nodes.



中國移動香港 中國移動 China Mobile

## 低空經濟網絡安全
## CMHK: Cybersecurity for low-altitude economy

香港的「低空經濟行動計劃」正推動先進航空技術融入城市交通、物流及緊急應變服務，致力將本港定位為區域創新樞紐。雖然此舉帶來了效率提升、產業增長及公共服務優化等裨益，但該領域亦面臨複雜的「雙重威脅」。除了傳統的網絡攻擊（如訊號干擾及 GPS 欺騙）外，業界還需應對未經授權的「黑飛」及無人機群等操作風險。這些因素交織形成「空中暗礁」——即隱蔽且混亂的危險，可能導致設備被劫持，構成嚴重的公共安全風險。

Hong Kong's Low-Altitude Economy Action Plan is driving integration of advanced aviation technologies into urban mobility, logistics, and emergency response, positioning the city as a regional hub for innovation. While benefits include efficiency gains, industry growth, and enhanced public services, the sector also faces a complex "dual threat." Beyond traditional cyberattacks—such as signal jamming and GPS spoofing—the sector contends with operational hazards like unauthorised "black flights" and drone swarms. These combine to create "air reefs"—hidden, chaotic dangers that can lead to hijacked devices and severe public safety risks.

### 技術與基礎設施挑戰 Technical & Infrastructure Challenges

空中物聯網設備主要的漏洞在於硬件本身。與功能強大的手提電腦不同，空中物聯網設備的處理能力及電池壽命有限。它們無法在不耗盡飛行電力的情況下，運行保護系統所需的繁重軍用級加密程序。這迫使營運商使用較輕量但安全性較弱的防護措施，令無線連接暴露於風險之中。此外，隨著數據在無人機、商業平台及監管系統之間傳輸，風險亦隨之倍增——不同系統之間的每一次「交接」都可能產生黑客可利用的潛在洩漏點。

The primary vulnerability of aerial IoT devices lies in the hardware itself. Unlike powerful laptops, aerial IoT devices have limited processing power and battery life. They simply cannot run the heavy, military-grade encryption needed to protect them without draining their power mid-flight. This forces operators to use lighter, weaker security, leaving wireless links exposed. Additionally, the risk is compounded as data jumps between drones, commercial platforms, and regulatory systems—every "handover" between these different systems creates a potential leak point that hackers can exploit.

### 偵測缺口 The Detection Gap

現有的防禦系統之所以不足，是因為它們是為封閉空間而非開放空域而設計。在廣域環境中，傳統感測器難以全方位掃描廣闊的距離。摩天大樓等實體障礙物會形成「訊號盲區」，阻擋訊號傳輸，讓隱蔽的攻擊得以避過偵測。此外，城市中混亂的環境會引發持續的誤報——將無害的無線電雜訊（如 Wi-Fi 或基站訊號）誤判為威脅——這會令營運商對潛伏在空中的真實危險視而不見。

Current defence systems are failing because they are designed for closed rooms, not open skies. In a wide-area environment, traditional sensors struggle to scan vast distances in every direction. Physical obstacles like skyscrapers create "shadow zones" where signals are blocked, allowing stealthy attacks to slip through undetected. Furthermore, the chaotic environment of a city triggers constant false alarms—mistaking harmless radio noise (like Wi-Fi or cell towers) for threats—which blinds operators to the real dangers lurking in the air.

### 韌性之路 Path to Resilience

為應對這些威脅與挑戰，作為低空經濟網絡安全的關鍵參與者，中國移動香港構建了「1+1+N」低空能力體系。中國移動香港的 5G-A ISAC基站結合了可靠通訊與空域異常偵測功能，能準確識別未經授權的無人機，該技術已在全運會香港賽區證實有效。此外 Hubble-1 5G 終端具備硬件級高級加密功能，為端到端可信低空網絡奠定基礎。

To address these threats and challenges, as a key participant in low-altitude economic cybersecurity, CMHK builds a "1+1+N" low-altitude capability system. CMHK's 5G-A ISAC base station combines reliable communications with airspace anomaly detection, accurately identifying unauthorised drones—proven effective in the National Games Hong Kong division. The Hubble-1 5G terminal features hardware-level advanced encryption, underpinning end-to-end trusted low-altitude networks.



## Web3與區塊鏈安全挑戰
## Web3 and Blockchain Security Challenges

### 引言 Introduction

Web3與區塊鏈技術在加密貨幣領域的迅速普及，衍生出一系列有別於傳統中心化系統的網絡安全挑戰。根據CertiK報告[8]，2025年全球共錄得630宗Web3安全事件，造成約33.5億美元損失，平均每次事件損失532萬美元。去中心化架構下，交易的偽匿名性、智能合約的不可逆性，以及用戶自行託管資產的責任轉移，均為網絡安全專業人員、監管機構及執法部門帶來了前所未有的難題。

The rapid adoption of Web3 and blockchain technologies, particularly in the realm of cryptocurrency, has introduced cybersecurity challenges fundamentally different from those of traditional centralised systems. According to a CertiK report[8], 630 Web3 security incidents were recorded worldwide in 2025, resulting in losses of approximately US$3.35 billion, with an average loss of US$5.32 million per incident. The pseudo-anonymity of transactions, the irreversibility of smart contracts, and the shift of security responsibility to end-users present unprecedented challenges for security professionals, regulators, and law enforcement.

### 智能合約漏洞持續構成重大威脅
### Smart Contract Vulnerabilities Remain a Critical Threat

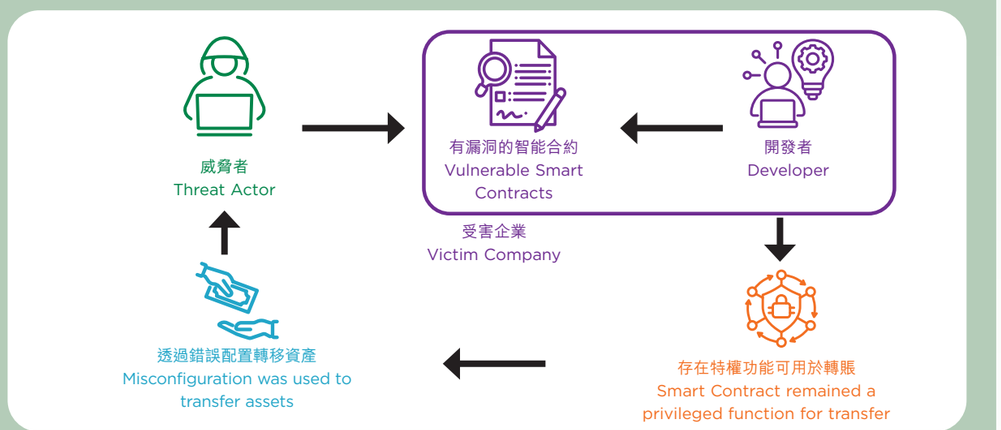
智能合約奉行「代碼即法律」的原則，一經部署便難以修改，與可持續更新的傳統軟件截然不同。程式邏輯錯誤、存取權限配置不當、未經審查的外部調用，以及審計測試不足等問題，往往導致不可逆轉的資金損失。有研究針對2020至2025年間曾遭攻擊的智能合約進行模擬測試，成功重現了過半數的攻擊場景，並在模擬環境中盜取超過5億美元的資金，反映智能合約的安全隱患依然嚴峻[9]。

Unlike traditional software with continuous updates, smart contracts operate on the principle of "Code is Law," making them extremely difficult to modify once deployed. Logic errors, misconfigured access controls, unchecked external calls, and insufficient auditing frequently lead to irreversible financial losses. A research study that tested previously exploited smart contracts from 2020 to 2025 successfully replicated over half of the attacks in simulated environments, extracting more than US$500 million in simulated stolen funds, highlighting the persistent severity of smart contract vulnerabilities[9].

### 個案六 Case Study 6 加密扣帳卡漏洞利用
### Crypto Debit Card Exploit

2025年2月，一間加密貨幣扣帳卡公司發生保安事故，導致損失4 950 萬枚 USDC。經調查後發現，該事件的根本原因在於開發人員於部署智能合約後未及時更新相關存取權限，導致原本應受限的特權功能持續暴露於外。攻擊者利用此配置疏漏，操作殘留的管理權限，成功操縱並轉移了該項目的大量資產。此案例揭示，存取權限配置錯誤至今仍是智能合約領域中最為常見且具高破壞力的安全風險之一。

In February 2025, a cryptocurrency debit card company experienced a security breach, resulting in a loss of 49.5 million USDC. Our investigation found that the root cause of this incident lay in the developer's failure to update access rights after deploying the smart contract, which left privileged functions persistently exposed. Leveraging this configuration oversight, the attacker manipulated the residual administrative permissions to successfully control and drain a substantial portion of the project's assets. This case underscores that access-right misconfiguration remains one of the most prevalent and high-impact security risks in the realm of smart contracts.




[8] CertiK. (2025, December 23). Hack3d: The Web3 security report 2025. https://www.certik.com/zh-CN/resources/blog/hack3d-the-web3-security-report-2025
[9] "AI agents find $4.6M in blockchain smart contract exploits", Anthropic, published on 2025-12-01, URL: https://red.anthropic.com/2025/smart-contracts/

### 私人密碼匙竊取與惡意軟件攻擊日趨猖獗
### Private Key Theft and Malware Attacks on the Rise

2025年，針對加密貨幣助記詞及私人密碼匙的竊取手法愈趨精密。攻擊者常以假冒視像會議應用程式、木馬安裝程式、瀏覽器惡意擴充功能或仿冒錢包程式作為攻擊媒介，並透過釣魚手段誘使目標安裝惡意軟件或洩露敏感資訊。Web3平台的員工及外判開發人員尤其容易成為攻擊目標。Lazarus團伙更於年內部署新型惡意軟件，專門滲透開發環境以竊取憑證，進一步加劇Web3生態的安全威脅。

In 2025, techniques for stealing cryptocurrency seed phrases and private keys grew increasingly sophisticated. Attackers commonly used fake virtual meeting applications, trojan installers, malicious browser extensions, and counterfeit wallet apps as attack vectors, employing phishing tactics to trick targets into installing malware or disclosing sensitive information. Employees and outsourced developers at Web3 platforms were particularly vulnerable. The Lazarus Group further escalated threats by deploying new malware strains specifically designed to infiltrate development environments and steal credentials.

### 合規與執法面臨全新挑戰
### Emerging Compliance and Enforcement Challenges

不少去中心化金融協議以無需許可的模式運作，用戶無需通過身份認證核查即可交易，令全球打擊洗錢及恐怖分子資金籌集（AML/CTF）框架面臨嚴峻考驗。區塊鏈網絡遍佈全球數千個節點，難以確定哪一司法管轄區的法律適用於特定交易，客觀上為犯罪分子提供了「監管套利」的空間，使其得以在法律環境最寬鬆的地區運作。

與此同時，兩股相互角力的趨勢正在浮現。一方面，愈來愈多區塊鏈在協議層面內建資產凍結功能，以配合合規需求，逐步將傳統金融的管控機制引入去中心化領域。另一方面，隨著穩定幣監管法規及機制逐步落實，非法交易正加速轉向即時通訊軟件群組、黑市「樓上店」等非正式的點對點渠道，進一步增加執法機構的監控及偵查難度。

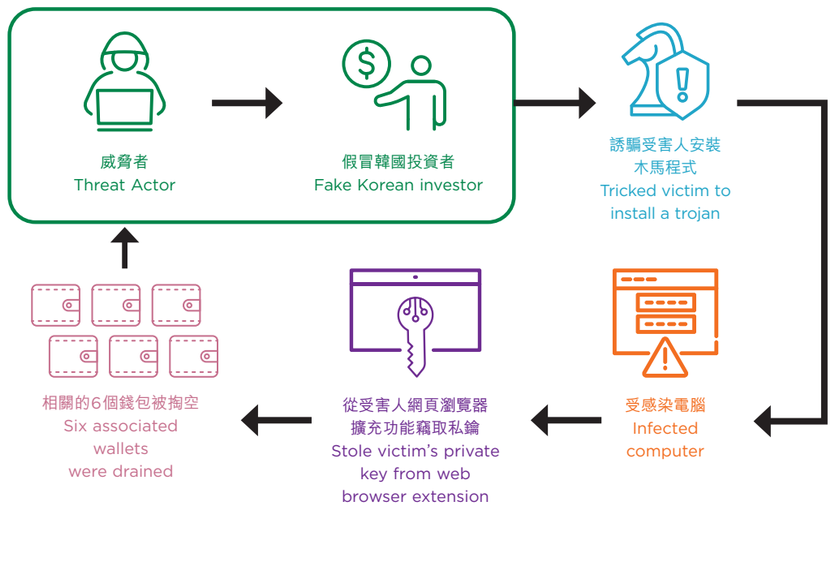
Many DeFi protocols operate on a permissionless basis, enabling users to transact without standard identity verification. This creates significant blind spots for regulators, undermining global Anti-Money Laundering and Counter-Financing of Terrorism (AML/CTF) frameworks. Blockchain networks are distributed across thousands of nodes worldwide, making it exceptionally difficult to determine which jurisdiction governs a specific transaction. This ambiguity enables regulatory arbitrage, where criminals exploit the most lenient legal environments.

Two countervailing trends are emerging simultaneously. On one hand, a growing number of blockchains are embedding protocol-level asset freezing capabilities to meet compliance demands, gradually introducing traditional financial controls into the decentralised space. On the other hand, as stablecoin regulations and mechanisms are progressively implemented, illicit trading is increasingly migrating to informal peer-to-peer channels such as instant messaging application groups and black market “upstairs” shops, further complicating law enforcement monitoring and investigation.

## 個案七 Case Study 7 透過木馬惡意軟件竊取私鑰
## Private Key Theft via Trojan Malware

本案涉及一名香港 DeFi 平台創辦人，因將所有私鑰儲存於瀏覽器內，導致平台其後遭受黑客入侵。2025年9月，其使用的手提電腦感染惡意軟件，致使六個關聯錢包被掏空，損失約3,200 萬枚代幣，價值相當於200萬美元。經調查發現，部分被盜資金在不同加密貨幣交易所被成功凍結，其餘資金則透過混幣器進行洗錢。進一步溯源顯示，攻擊過程中使用的手續費來自一個與惡名昭彰的Lazarus 團伙所使用的錢包相關聯的地址。經追溯惡意軟件的來源後，發現一名假冒的韓國投資者曾以合作為名，誘騙事主下載並安裝了一個惡意即時通訊應用程式，從而植入木馬。

This case involves a Hong Kong-based DeFi platform founder who stored all private keys within the browser, leading to the subsequent hacking of the platform. In September 2025, the founder’s laptop was infected with malware, resulting in six associated wallets being drained, with losses amounting to approximately 32 million tokens, equivalent to US$2 million. Post-incident investigation revealed that a portion of the stolen funds was successfully frozen on different cryptocurrency exchanges, while the remaining funds were laundered through the mixer. Further tracing indicated that the gas fees used in the attack originated from an address linked to wallets utilised by the notorious Lazarus Group. The malware was traced to a fake Korean investor who, under the guise of collaboration, tricked the victim into downloading and installing a malicious instant messaging application, thereby deploying the trojan.




## Beosin 區塊鏈安全新興威脅
## Blockchain security emerging threat

### 錢包安全問題依然嚴峻 Wallet Security Issues Remain Severe

據Beosin安全年報顯示，2025年虛擬資產行業因網絡攻擊而導致的總損失約33.75億美元，交易所成為黑客主要攻擊目標，9家交易所主要因錢包安全問題被攻擊，共損失17.65億美元，佔全年損失的52.3%。2025 年 2 月，Bybit 因其多簽錢包被植入惡意代碼，簽署人在簽署轉賬交易時未發現交易內容被篡改，導致14.5億美元損失。黑客快速通過LI.FI，THOR等跨鏈平台，Tornado Cash等混幣平台，以及無KYC的交易所進行資金轉移，僅3.8%被盜資金被追回，成為迄今為止 Web3歷史上損失最大的安全事件。

According to the Beosin Annual Security Report, the virtual asset industry suffered total losses of approximately US$3.375 billion in 2025 due to cyberattacks, where exchanges have become the primary targets for hackers. Nine exchanges were attacked primarily due to wallet security issues, resulting in a combined loss of US$1.765 billion, which accounts for 52.3% of the total annual losses. In February 2025, Bybit suffered a loss of US$1.45 billion after malicious code was injected into its multi-signature wallet. The signers failed to detect that transaction details had been tampered with during the signing process. Hackers rapidly transferred funds through cross-chain platforms like LI.FI and THOR, mixing services like Tornado Cash, and exchanges without KYC. Only 3.8% of the stolen funds were recovered, making this the largest security incident in Web3 history to date.

### 虛擬資產作為洗錢等犯罪主要資金通道
### Virtual Assets as a Primary Channel for Money Laundering and Crimes

2025年，虛擬資產已逐漸成為全球黑灰產洗錢與非法交易的主要工具，並衍生出「黑客攻擊+跨鏈混幣」、「網上詐騙+擔保平台黑灰產業鏈」等高隱蔽性的犯罪形式。根據Beosin安全年報顯示，全球最大的混幣平台Tornado Cash年交易總額超過22億美元；匯旺、新幣等主流擔保平台的擔保金年總額超過87億美元；主流跨鏈橋平台的年總流水超過千億美元。

In 2025, virtual assets have gradually become the primary tool for global black and grey market money laundering and illicit transactions. This has spawned highly concealed forms of crime, such as “Hacking + Cross-chain Mixing” and “Online deception+ Guarantee Platform Black/Grey Industry Chains.” According to the Beosin Annual Security Report, Tornado Cash, the world’s largest mixing platform, saw an annual transaction volume exceeding US$2.2 billion; the total annual guarantee amounts on mainstream guarantee platforms like Huione and Xinbi exceeded US$8.7 billion; and the annual turnover of mainstream cross-chain bridge platforms surpassed US$100 billion.

### 單一反洗錢工具難以應對洗錢問題
### Single Anti-Money Laundering (AML) Tools Are Insufficient to Tackle Money Laundering

在當前全球虛擬資產監管不斷強化的趨勢下，85個國家和地區已推行虛擬資產牌照制度，明確要求VASP建立完善的安全體系並運用KYT等反洗錢技術，以增強其安全性、預防洗錢風險。然而在實踐層面，多數VASP僅依賴單一KYT工具，難以全面覆蓋跨境、跨司法轄區的複雜洗錢風險。因此，有必要推動採用「混合」KYT解決方案，透過多元技術互補，系統性地提升VASP的整體反洗錢能力。

監管科技企業、監管機構與執法部門應該進一步深化協作，共同防範網絡犯罪、管控新興技術風險，並透過提升業界與公眾的安全意識，攜手構建更加安全、更具韌性的數字生態。

Amid the current trend of strengthening global virtual asset regulation, 85 countries and regions have implemented virtual asset licensing systems. These explicitly require Virtual Asset Service Providers (VASPs) to establish comprehensive security frameworks and utilise AML technologies, such as Know-Your-Transaction (KYT), to enhance security and prevent money laundering risks. However, in practice, most VASPs rely on a single KYT tool, which struggles to comprehensively cover complex money laundering risks that span borders and jurisdictions. Therefore, it is necessary to promote the adoption of “hybrid” KYT solutions to elevate the overall AML capabilities of VASPs systematically through the complementarity of diverse technologies.

RegTech enterprises, regulatory bodies, and law enforcement agencies should further deepen their collaboration to jointly prevent cybercrime and manage risks associated with emerging technologies. By raising security awareness among both the industry and the public, we can work together to build a safer and more resilient digital ecosystem.

# 網絡資產安全評估
## Internet-Facing Assets Security Assessment

香港是國際知名的智慧城市、全球商貿和金融中心、以及國際航運和貿易樞紐，同時也是重要和專業服務核心基地，高度依賴其先進的運輸、通訊、金融及公共基礎設施系統。一旦核心服務遭受網絡攻擊而中斷，不僅會造成重大經濟損失，更可能引發公共安全危機，並損害國際社會對本港的信心。

Hong Kong, recognised as a smart city and a global leader in commerce and finance, serves as a vital hub for international shipping and trade, as well as a centre for essential professional services. These functions rely heavily on its advanced transportation, telecommunications, financial, and utility infrastructures. Any disruption to these core services due to cyberattacks could result in significant economic losses, pose risks to public safety, and undermine international confidence in the city.

有見全球重要基礎設施持續遭受網絡威脅，網罪科定期進行「網絡資產安全評估」。這項安全評估旨在偵測重要基礎設施中，面向互聯網的網絡資產（例如URLs、域名及IP地址）裡可能存在的系統安全漏洞，以確保這些重要網絡資產的安全與韌性。

In view of the persistent cyber threats targeting critical infrastructures worldwide, CSTCB regularly conducts Internet-facing Assets Security Assessments, which aim to identify potential system vulnerabilities in the Internet-facing assets of critical infrastructures (such as URLs, domain names, and IP addresses) to ensure their security and resilience.


2025年，網罪科針對香港重要基礎設施的網絡資產共進行逾10萬次評估，發現當中7.8%存在不同程度的系統安全漏洞，較2024年的5%略有上升，整體網絡資產系統安全狀況與去年相近。透過現有的通報機制，所有被識別的系統安全漏洞均已及時修補，受影響機構亦已全面提升系統防護水平，凸顯了持續進行主動評估和監測的重要性。

In 2025, CSTCB conducted over 100,000 assessments on internet-facing assets of critical infrastructures in Hong Kong and found that 7.8% of these assets had varying degrees of system vulnerabilities, representing a slight increase from the 5% recorded in 2024. Overall, the security posture of internet-facing assets remained similar to that of the previous year. Through the established notification mechanism, all identified system vulnerabilities were promptly patched, and the affected organisations have substantially enhanced their system security posture, underscoring the importance of ongoing proactive assessment and monitoring.

在逾8 000個已識別的系統安全漏洞中，95%被歸類為中低風險，其餘5%則被歸類為極高及高風險級別，主要包括憑證外洩或盜用、可被騎劫的子域名，以及被暴露的雲端儲存服務。

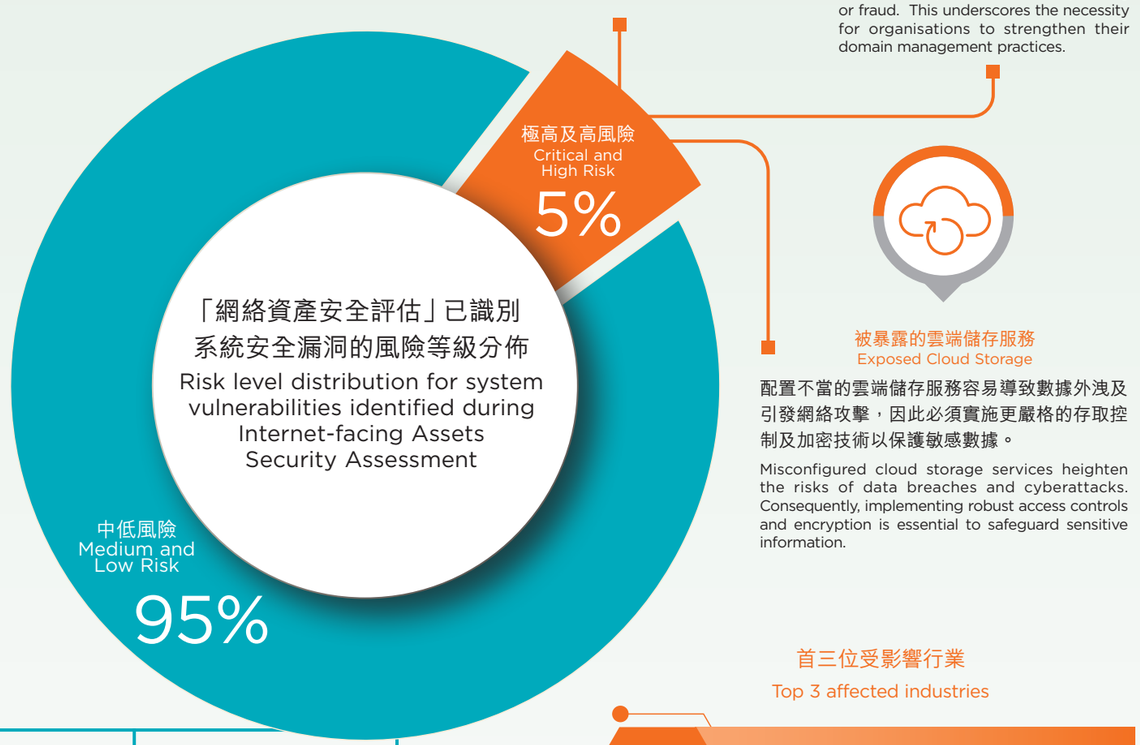
Of the more than 8,000 system vulnerabilities identified, 95% were classified as medium and low risk, while the remaining 5% were categorised as critical and high risk. These higher-risk vulnerabilities primarily included credential leakage or compromise, hijackable subdomains, and exposed cloud storage services:

**中低風險漏洞**
**Medium and Low Risk Vulnerabilities**

這漏洞讓威脅者直接發動網絡攻擊的可能性相對較低，但仍可被利用於偵察活動，為進一步網絡攻擊創造條件。
These vulnerabilities are less likely to enable direct cyberattacks but may still be exploited for reconnaissance activities, potentially paving the way for further cyberattacks.

**極高及高風險漏洞**
**Critical and High Risk Vulnerability**

這類漏洞極有可能讓威脅者能夠直接發動網絡攻擊，並可能對重要基礎設施的正常營運構成重大影響。
These vulnerabilities could allow threat actors to launch cyberattacks directly and may pose a significant risk to the normal operation of critical infrastructures.




**憑證外洩或盜用**
**Credential Leakage / Compromise**

員工或公眾的登入憑證一旦外洩或被盜用，攻擊者即可藉此未經授權接達關鍵系統，從而構成重大安全威脅。
Credential Leakage or Compromise: Leaked or stolen credentials, whether from staff or the public, pose a major security threat by enabling attackers to gain unauthorised access to critical systems.

**可被騎劫的子域名**
**Hijackable Subdomains**

閒置或管理不善的子域名可能遭攻擊者接管並用於進行釣魚攻擊或詐騙活動，此類情況反映機構必須加強域名管理措施。
Hijackable Subdomains: Unused or poorly managed subdomains can be taken over by attackers and exploited for malicious purposes, such as phishing or fraud. This underscores the necessity for organisations to strengthen their domain management practices.

**被暴露的雲端儲存服務**
**Exposed Cloud Storage**

配置不當的雲端儲存服務容易導致數據外洩及引發網絡攻擊，因此必須實施更嚴格的存取控制及加密技術以保護敏感數據。
Misconfigured cloud storage services heighten the risks of data breaches and cyberattacks. Consequently, implementing robust access controls and encryption is essential to safeguard sensitive information.

**郵件伺服器被列入黑名單**
**Mail server blacklisting**

重要基礎設施所使用的郵件伺服器被列入黑名單，顯示該伺服器可能已遭入侵並成為殭屍網絡的一部分。
When critical infrastructures' email servers are blacklisted, it indicates that they may have been compromised and incorporated into a botnet.

**證書授權問題**
**Certificate authority issues:**

使用無效或過時的網絡安全證書。
The use of invalid or outdated cybersecurity certificates.

**保密插口層/傳輸層保安問題**
**SSL/TLS issues**

面向互聯網的網絡資產採用了較弱的加密套件和密鑰。
Internet-facing assets utilise weak cipher suites or cryptographic keys.

**可被利用的端口**
**Exploitable ports**

未受限制的端口可能被利用以達成惡意目的。
Unrestricted ports can be exploited for malicious purposes.

**暴露的網頁介面**
**Exposed web interface**

內部或敏感系統被托管於公開可訪問的網頁上（例如用於系統控制的登入頁面）。
Internal or sensitive systems are hosted on a publicly accessible webpage (e.g. a login page for system control).

**首三位受影響行業**
**Top 3 affected industries**

1. 能源 Energy
2. 銀行及金融服務 Banking & Financial Services
3. 通訊 Communications

# 網絡安全問卷調查
# Cybersecurity Survey

網罪科每年均會進行抽樣問卷調查，以評估本港重要基礎設施營運者及大型機構的網絡安全意識及應變準備狀況。在2025年，我們訪問了來自銀行及金融業、政府部門、通訊業、公共事業及運輸業等多個行業的重要基礎設施營運者及大型機構。以下為本年度問卷調查的主要發現，涵蓋威脅形勢、警覺性及應變準備、網絡安全預算，以及人工智能應用四大範疇。

CSTCB conducts an annual sample survey to assess the cybersecurity awareness and preparedness of Hong Kong's critical infrastructure operators and major organisations. In 2025, we have interviewed critical infrastructure operators and major organisations from different industries, including banking and finance, government departments, communications, public utilities and transportation. The following presents the key findings of this year's survey, covering four areas: the threat landscape, alertness and preparedness, cybersecurity budget, and AI adoption.

## 威脅形勢
## Threat Landscape

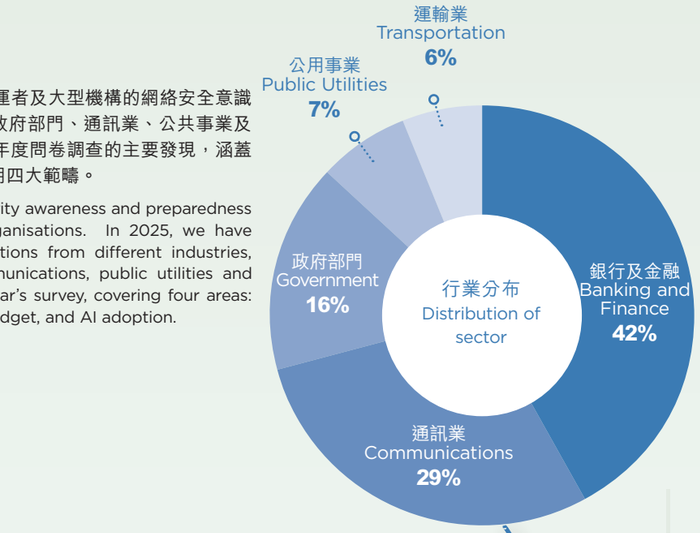
調查結果顯示，重要基礎設施及大型機構面對網絡威脅的頻率正持續上升。36%受訪機構表示在2025年曾遭遇「頻繁」或「非常頻繁」的網絡威脅，比例較前一年增加了16%。遭受網絡威脅頻率最高的三個行業分別是銀行及金融業（42%）、通訊業（29%）和政府部門（16%），與 2024 年的調查結果大致相符。

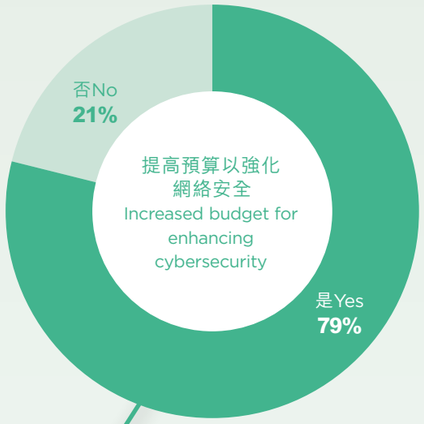
The survey results indicated a sustained increase in the frequency of cyber threats faced by critical infrastructures and major organisations. 36% of organisations reported experiencing "frequent" or "very frequent" cyber threats in 2025, representing a 16% increase compared to the previous year. The top three sectors facing the highest frequency of cyber threats were banking and finance (42%), communications (29%), and government departments (16%), which aligns closely with the 2024 survey findings.

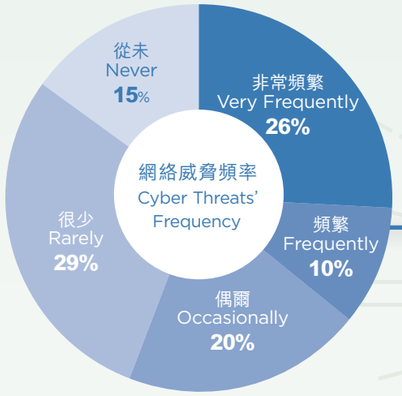
## 警覺性及應變準備
## Alertness & Preparedness

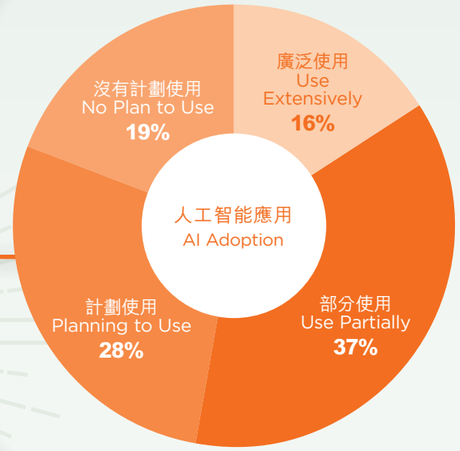
絕大多數受訪者對自身網絡安全狀況仍持樂觀評價，約85%自評對網絡威脅維持著高度警覺，約81%認為自身具備充分的網絡安全應變準備。雖然調查結果顯示受訪機構對自身應變準備度評價頗高，但同時也反映了各機構對抵禦日益複雜網絡攻擊的能力抱有更審慎的態度。透過審慎的自我評估，機構能夠更精準地分配資源，以持續提升網絡安全狀況。

The vast majority of respondents continued to hold an optimistic view of their cybersecurity posture. Around 85% self-rated as maintaining high alertness to cyber threats, and about 81% believed they had adequate cybersecurity preparedness. While these results indicate a generally high self-assessment of readiness, they also reflect a more cautious outlook among organisations regarding their ability to defend against increasingly sophisticated cyberattacks. Through prudent self-assessment, organisations can allocate resources more strategically and thereby continuously enhance their cybersecurity posture.

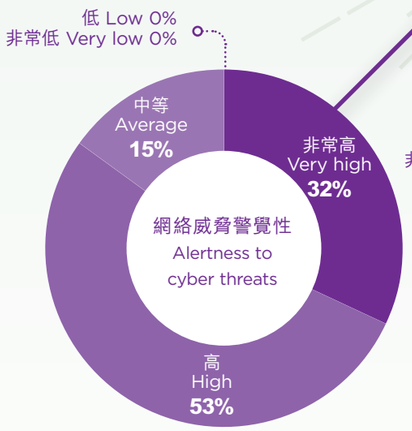


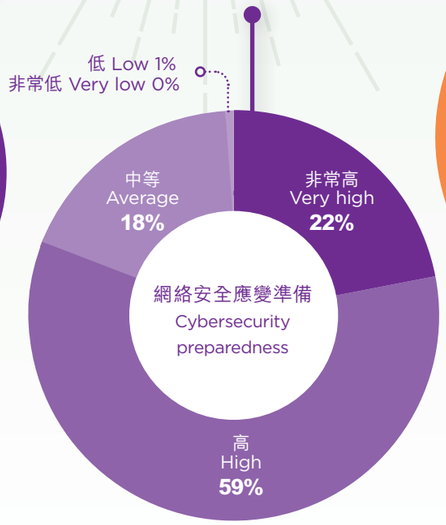



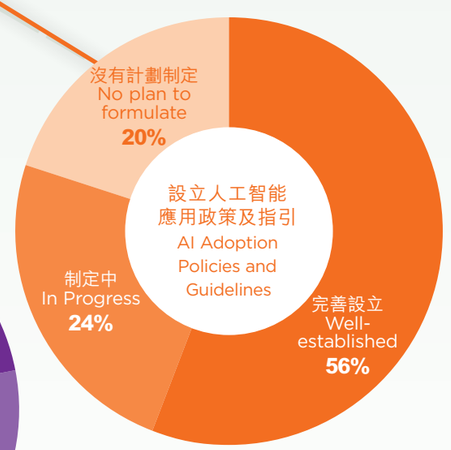








## 網絡安全預算
## Cybersecurity Budget

因應日益嚴峻的網絡威脅，各機構正積極投入更多資源以加強網絡安全防護。調查顯示，2025年有79%的受訪機構已增加相關預算，用於強化網絡安全措施。

In response to the increasingly severe cyber threats, organisations were actively allocating more resources to strengthen their cybersecurity defences. The survey shows that in 2025, 79% of responding organisations had increased their budgets for enhancing cybersecurity measures.

## 人工智能應用
## AI Adoption

超過八成受訪機構表示已經或計劃利用人工智能來提升網絡安全。同時，有80%的受訪者表示已制定或正在制定人工智能應用政策及指引。

More than 80% of responding organisations indicated that they have already utilised or plan to utilise AI to enhance cybersecurity. Concurrently, 80% of respondents stated that they have either established or are in the process of establishing policies and guidelines for AI application.

問卷調查結果顯示，隨著各機構面臨日益頻繁且複雜的網絡攻擊，除了增加資源以提升網絡安全，機構亦積極研究利用前沿科技加以應對，例如人工智能技術。雖然採用新科技對於建立強大而穩健的防禦體系至關重要，但亦可能引入新的系統安全與治理風險。網絡安全是企業持續發展的基石。無論規模大小，所有機構都必須持續提升防禦能力，以確保企業營運安全。

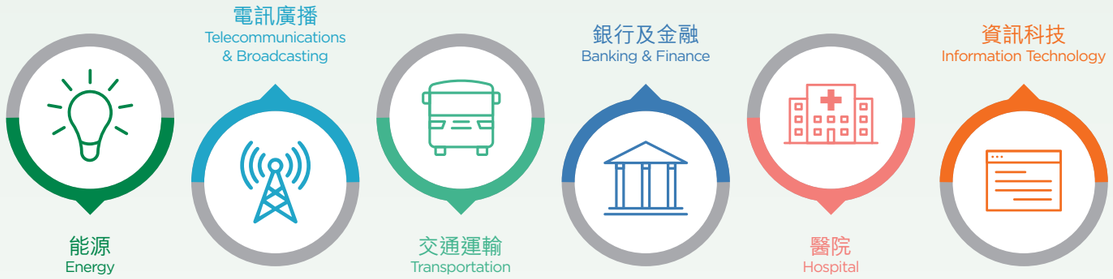
The survey results indicated that as organisations faced more frequent and complex cyberattacks, they were not only devoting more resources towards enhancing cybersecurity but were also actively exploring the adoption of cutting-edge technologies, including AI, to respond to these threats. While adopting new technologies is essential for building strong and robust defences, it may also introduce new system security and governance risks. Cybersecurity serves as the cornerstone of sustainable business development. Regardless of their size, all organisations must continuously enhance their defensive capabilities to ensure the security of operations.

# 《關鍵基礎設施的電腦系統安全挑戰》
# Computer-system Security Challenges Faced by Critical Infrastructures

關鍵基礎設施（電腦系統安全）專員辦公室
The Office of the Commissioner for Critical Infrastructure (Computer-system Security)

2025年的多宗事故再次響起警號：去年3月，烏克蘭國營鐵路遭遇網絡攻擊，導致網上售票服務癱瘓，乘客大排長龍，部分與貨運相關的網上服務亦遭受波及；同年9月，歐洲多個機場的自助登機服務中斷，歐盟網絡安全機構指事件涉及針對第三方供應商的勒索軟件攻擊，這反映一旦共用的供應商遭受攻擊，影響可迅速擴散，甚至演變成系統性風險。

Multiple incidents in 2025 have once again sounded the alarm. In March 2025, a cyberattack knocked out online ticketing for Ukraine's state railway, forcing passengers into long queues, while some freight-related online services were also affected. In September 2025, disruptions to automated check-in systems across multiple European airports were linked by the EU's cybersecurity agency to a ransomware attack targeting third party services, underscoring how shared vendors can become systemic points of failure.




香港的關鍵基礎設施橫跨多個界別，遍及能源、電訊廣播、交通運輸、銀行及金融、醫院和資訊科技等領域，它們大多依賴安全可靠的電腦系統提供服務。本地一旦發生電腦安全事故，可能對社會帶來連鎖反應，繼而影響市民日常生活。對關鍵服務提供者而言，訊息很清楚：韌性不能依靠假設，而要靠日常落實與持續驗證，做到未雨綢繆。

Hong Kong's critical infrastructures span multiple sectors, including energy, telecommunications and broadcasting, transportation, banking and finance, hospitals, and information technology. They largely rely on secure, reliable computer systems to deliver essential services. In the event of a computer security incident, it could trigger a chain reaction and subsequently impact citizens' daily lives. For critical service providers, the message is clear: resilience cannot be assumed; it must be implemented day to day and continuously validated - fixing the roof before it rains.

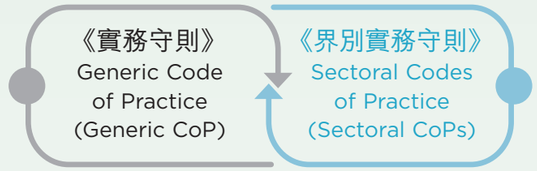
為進一步提升電腦系統安全的整體水平，《保護關鍵基礎設施（電腦系統）條例》（第653章）（「《條例》」）已於2026年1月1日生效，以訂立清晰的法定框架及務實的指引。《條例》旨在向被指定的「關鍵基礎設施營運者」施加法定責任，確保他們採取適當措施保護其電腦系統，減低因網絡攻擊導致關鍵服務被干擾或破壞的風險，從而維持香港社會的正常運作和市民的正常生活。《條例》訂明三類法定責任：架構、預防，以及事故通報及應對，以一致而清晰的要求提升營運者的整體準備程度。

To further enhance the overall computer-system security, the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) has come into effect on 1 January 2026, setting a clear statutory framework and practical implementation guidelines. The ordinance aims to impose statutory obligations on designated critical infrastructure operators to ensure they take appropriate measures to protect their computer systems, thereby reducing the risk of disruption or damage to critical services caused by cyberattacks, in order to safeguard the normal functioning of Hong Kong society and the daily lives of its citizens. The ordinance stipulates three categories of statutory obligations: organisational, preventive, and incident reporting and response. These obligations raise the overall preparedness through clear and consistent requirements.



經過與業界持續溝通，保安局亦先後推出通用《實務守則》及《界別實務守則》。《實務守則》以務實可行為原則，把法例要求轉化為可落實、可驗證的基線要求，協助營運者按部就班建立及提升保護電腦系統的能力。《實務守則》同時透過管治安排，例如要求由董事局或高層核准電腦系統安全管理計劃，推動企業由上而下將電腦系統安全融入日常管理和營運決策。《實務守則》參考成熟的國家標準、國際標準及業界良好作業模式，並按香港的營運環境作出調整。在此之上，《界別實務守則》則因應個別界別的行業慣例、技術架構或營運環境的特別需要，提供更貼近實際的建議，確保指引可行到位。

Following continued engagement with the trade, the Security Bureau has issued a Generic Code of Practice (Generic CoP) and Sectoral Codes of Practice (Sectoral CoPs). The Generic CoP is designed to be pragmatic and practicable, translating statutory requirements into an actionable baseline that can be implemented and verified, helping operators build and enhance their capability to protect computer systems step by step. It also promotes the integration of computer-system security into daily management and operational decisions through governance requirements, such as by requiring the board or senior management to endorse the computer-system security management plan. The Generic CoP draws on mature national and international standards and recognised industry good practices, and has adapted to Hong Kong's operating context. Furthermore, the Sectoral CoPs provide more tailored recommendations to reflect sector-specific practices, technical architectures and operational needs, ensuring the guidance is workable and fit for the purpose.




此法律框架的價值不止於「合規」，更在於把網絡韌性融入日常營運，即從企業管治、變更管理、系統加固、風險監測、供應鏈風險管理、事故演練、應變，以至復原，逐步建立一套可持續的做法，並透過《實務守則》和《界別實務守則》的建議，把良好實踐延伸至外判服務供應商。

The value of this legislative framework goes beyond mere compliance. It embeds cyber resilience into day-to-day operations. This encompasses corporate governance, change management, system hardening, risk monitoring, supply chain risk management, incident drills, response and recovery. It progressively establishes sustainable practices and extends good practices to outsourced service providers through recommendations in the Generic CoP and Sectoral CoPs.

關鍵基礎設施（電腦系統安全）專員辦公室會與指定當局、執法部門、監管機構共同協作，並與營運者、服務供應商及各持份者攜手，築起更完善的多層防護，提升香港的整體電腦安全。

The Office of the Commissioner for Critical Infrastructure (Computer-system Security) will collaborate with designated authorities, law enforcement agencies and regulators, and join hands with operators, service providers and various stakeholders to build a robust multi-layer defence to enhance Hong Kong's overall computer security.

關鍵基礎設施（電腦系統安全）專員辦公室發布的《實務守則》明確訂明營運者須履行三大法定責任。

The Code of Practice issued by the Office of the Commissioner for Critical Infrastructure (Computer-system Security) clearly sets out three categories of statutory obligations that operators are required to fulfil.

架構責任：包括設立專責安全管理單位、維持本地辦事處，以及就營運者相關變更作出通報；

Organisational obligations: including the establishment of a dedicated security management unit, the maintenance of a local office, and the notification of relevant changes concerning the operator;

預防責任：包括要求提交和實施安全管理計劃，以及定期進行風險評估及安全審核；

Preventive obligations: including the submission and implementation of a security management plan and the conduct of regular risk assessments and security audits;

事故通報與應對責任：涵蓋參與網絡安全演習、提交及實行應急計劃，以及於法定時限內通報安全事故。

Incident reporting and response obligations: including participation in cybersecurity drills, the submission and implementation of emergency response plans, and the reporting of security incidents within prescribed timeframes.

在此制度框架下，警方於執法與統籌協調方面擔當關鍵角色，負責調查涉及網絡攻擊或刑事成分的案件，支援重大事故的應對工作，並與保安局及相關監管機構保持跨部門協作，形成技術防護與執法保障並行的雙重防線。

Within this regulatory framework, the HKPF plays a pivotal role in enforcement and coordination. It is responsible for investigating cases involving cyberattacks or criminal elements, supporting the response to major incidents, and working in close collaboration with the Security Bureau and relevant regulators, thereby establishing a dual line of defence that integrates technical safeguards with law enforcement protection.

# 網絡安全建議
# Cybersecurity Mitigations

以下十項建議涵蓋本報告所識別的主要風險領域，為各機構提供一套統一、可操作的防護框架。
The following ten recommendations address the principal risk areas identified throughout this report, providing a unified, actionable defence framework.

## 1 以身份為核心的存取控制
## Identity-Centric Access Control

所有遠端及特權存取均應部署抗釣魚多重認證（如FIDO2/WebAuthn或基於PKI的方案），並實施基於裝置健康狀態、用戶風險評分及會話環境的條件式存取策略。機構應定期審查並停用閒置及預設管理帳戶，按既定周期更換存取密碼匙及憑證，並即時撤銷多餘權限。身份驗證流程應加入活體偵測技術（如隨機動作挑戰及三維深度感測）及多層驗證機制，以對抗深偽及人工智能偽造身份的攻擊手法。

All remote and privileged access should be protected by phishing-resistant MFA such as FIDO2/WebAuthn or PKI-based solutions, with conditional access policies evaluating device health, user risk score, and session context. Idle and default administrative accounts need regular review and disablement, access keys should be rotated on a defined schedule, and redundant privileges revoked promptly. Identity workflows should incorporate liveness detection (e.g. randomised challenge-response and 3D depth sensing) alongside multi-layered verification to counter deepfake and AI-fabricated document bypass attacks.

## 2 採用零信任架構
## Zero Trust Architecture Adoption

機構應在所有環境中採用零信任模式，持續驗證每個存取請求，並嚴格遵循最小權限原則。網絡須實施微分段策略，按功能及風險等級劃分區域以限制橫向移動。零信任理念同樣適用於軟件供應鏈及雲端平台，對所有外部依賴項預設為不可信，確保即使邊界防護被突破，攻擊者仍難以在內部自由移動。

Organisations should adopt a Zero Trust model across all environments, continuously verifying every access request and granting only minimum required privileges. Micro-segmentation should divide networks by function and risk level to restrict lateral movement. The same principles extend to the software supply chain and cloud platforms, treating all external dependencies as untrusted and ensuring attackers cannot move freely within internal environments even if perimeter defences are breached.

## 3 持續漏洞管理與修補
## Continuous Vulnerability and Patch Management

機構應建立以風險為導向的漏洞管理機制，優先處理CVSS 9.0以上的漏洞及面向互聯網的資產（包括網站應用系統、VPN閘道、防火牆韌體及關鍵第三方函數庫）。每季應對外部攻擊面進行探測掃描，主動識別影子資產。邊緣及物聯網裝置的韌體更新週期需加以維持，並訂閱供應商安全公告。已停止支援的系統須制定明確淘汰時間表，同時結合依賴性掃描工具持續監控供應鏈中的已知漏洞。

A risk-prioritised vulnerability and patch management programme should address critical vulnerabilities (CVSS 9.0+) and internet-facing assets first, including web applications, VPN gateways, firewall firmware, and critical third-party libraries. Quarterly external attack surface scans help identify shadow-exposed assets. Firmware update cycles for edge and IoT devices must be maintained with vendor advisory subscriptions. Clear decommissioning timelines should be defined for end-of-support systems, and dependency scanning tools integrated to monitor supply chain vulnerabilities continuously.

## 4 人工智能驅動的威脅偵測與回應
## AI-Augmented Threat Detection and Response

機構應部署結合人工智能的EDR及XDR方案，透過行為分析識別程序、API調用及網絡流量中的異常活動。端點、網絡及身份驗證遙測數據應整合至統一分流視圖，讓分析人員能關聯橫向移動信號。在電郵安全方面，應部署具備自然語言處理能力的閘道以偵測人工智能生成的釣魚訊息，並全面實施DMARC、DKIM及SPF。初步封鎖行動（如隔離端點及封鎖可疑連線）亦應盡可能自動化。


AI-augmented EDR and XDR solutions should detect anomalous activity through behavioural analytics across process behaviour, API call sequences, and network traffic patterns. Telemetry from endpoints, networks, and authentication should feed into a unified triage view for correlating lateral movement signals. Email gateways with natural language processing capabilities should detect AI-generated phishing and impersonation patterns, with full DMARC, DKIM, and SPF implementation. Initial containment actions such as endpoint isolation and connection blocking should be automated wherever possible.

## 5 集中化日誌管理與證據準備
## Centralised Log Management and Evidence Readiness

機構應建立集中化、防篡改的日誌儲存庫，至少保留九十天記錄，涵蓋認證事件、遠端存取會話、特權帳戶活動及雲端控制平面操作，建立端到端日誌管理。機構須核實第三方平台及SaaS供應商是否保存完整的操作日誌以支援事件調查。此外，應制定快速證據保全手冊，明確規定由誰、在什麼時限內擷取哪些鑑證數據，確保在封鎖行動覆蓋證據前完成取證。

A centralised, tamper-resistant log repository should be maintained with a minimum 90-day retention period, covering authentication events, remote access sessions, privileged account activities, and cloud control-plane operations to establish end-to-end governance. Organisations should verify that third-party platforms and SaaS providers retain system-level logs to support incident investigation. A rapid evidence-preservation playbook should specify who captures what forensic artefacts and within what timeframe, securing them before containment actions overwrite evidence.

# 網絡安全建議
# Cybersecurity Mitigations

## 6 備份韌性與復原能力
## Backup Resilience and Recovery

備份架構應以生產環境的身份驗證系統將被攻陷為前提來設計，備份憑證及存取路徑須完全獨立於網域。機構應維持至少一份不可變更或物理隔離的備份副本，配備自動完整性驗證機制。每年須針對全環境加密情景進行還原演練，並制定「最低可行業務」復原計劃，明確界定須優先復原的系統。備份伺服器須實施嚴格的網絡隔離，使其不可從一般端點直接存取。

Backup architecture should assume that production authentication infrastructure will be compromised, with backup credentials and access paths fully independent of the domain. At least one immutable or air-gapped backup copy should be maintained with automated integrity verification. Annual restore drills simulating full-environment encryption should be conducted, alongside a tested “minimum viable business” recovery plan identifying priority systems. Backup servers must remain unreachable from standard endpoints through strict network isolation.

## 7 第三方及供應鏈風險管治
## Third-Party and Supply Chain Risk Governance

機構應在整個供應商合作周期中持續執行盡職審查，訂立清晰的保安事故通報要求。準確的軟件物料清單（SBOM）應予建立並持續更新，以便在供應商遭入侵時迅速識別受影響範圍。開發實務應參照安全軟件開發框架（SSDF），建置流程須具備來源追溯及完整性驗證能力。非生產環境亦須納入安全治理範圍。SaaS平台的第三方應用程式授權應實施管理員預先批准機制，並定期檢視權限設定。

Lifecycle vendor risk management should include due diligence, ongoing assurance, and clear incident-notification requirements. An accurate SBOM should be maintained and continuously updated for rapid impact identification when a supplier is compromised. Development practices should follow the Secure Software Development Framework (SSDF) with provenance and integrity controls for builds and releases. Non-production environments must also fall within security governance scope. Admin pre-approval should be enforced for third-party application consent in SaaS platforms, with regular permission reviews.

## 8 網絡分段與攻擊面縮減
## Network Segmentation and Attack Surface Reduction

網絡應按功能及風險等級分段，將物聯網裝置、非生產環境及管理介面隔離於獨立的虛擬區域網絡，限制橫向流量。僅業務必需的服務方可對外暴露，管理介面須置於零信任存取架構後方。閒置的舊有通訊協定（如RTSP、ONVIF）及未受限制的端口應予停用或關閉。機構應維持物聯網裝置資產清單，監察異常對外連線行為以識別遭入侵裝置。所有遠端存取應整合至單一受監控閘道，配備完整會話記錄，並在網絡及端點層面封鎖所有未經批准的遠端工具。

Networks should be segmented by function and risk level, isolating IoT devices, non-production environments, and administrative interfaces on separate VLANs to restrict lateral movement. Only business-essential services should be externally exposed, with administrative interfaces behind Zero Trust controls. Legacy protocols such as RTSP and ONVIF should be disabled and unrestricted ports closed. An IoT asset inventory should be maintained and monitored for abnormal outbound connections. All remote access should be consolidated through a single monitored gateway with full session recording, and unapproved remote tools blocked at network and endpoint levels.

## 9 事故應變準備與測試
## Incident Response Preparedness and Testing

機構應制定全面的事故應變計劃，每年至少進行一次桌面演練，專門模擬備份遭破壞及攻擊者長期潛伏的勒索軟件情景。每個警報嚴重級別須指定負責人及明確通報時限，涵蓋非辦公時間安排。演練範圍應涵蓋加密資產事故（確保能即時通報以爭取凍結資金窗口）、供應鏈事故及涉及深偽技術的社交工程攻擊。人工智能驅動的攻擊手法亦應納入滲透測試及紅隊演練，以更新事故應變手冊。

Comprehensive incident response plans should be rehearsed at least annually, focusing on ransomware scenarios involving backup destruction and extended dwell time. Each alert severity tier should have a named owner with documented reporting timelines covering after-hours periods. Drills should extend to crypto-asset incidents (ensuring rapid notification to maximise fund-freezing windows), supply chain compromises, and social engineering using AI-generated phishing and deepfake voice. AI-driven attack vectors should be integrated into penetration testing and red-team exercises to identify gaps and update IR playbooks.

## 10 安全意識與人員培訓
## Security Awareness and Personnel Training

機構應定期為不同崗位員工提供針對性安全培訓，涵蓋識別人工智能生成的釣魚攻擊、深偽社交工程、偽冒應用程式及虛假合作邀請等新型手法，並透過定期釣魚及短訊模擬演習測試員工識別能力。機構應建立嚴格的軟件安裝審批流程，防止員工安裝木馬化應用程式。推動全機構範圍內的網絡安全文化同樣重要，確保資訊安全成為企業管治的核心議題。

Regular, role-specific training should cover AI-generated phishing, deepfake social engineering, counterfeit applications, and fraudulent collaboration requests. Periodic phishing and SMS simulation exercises should test and reinforce recognition skills. Strict software installation approval processes should prevent unwitting installation of trojanised applications. An organisation-wide cybersecurity culture should position security as a core governance matter.

# 網絡安全應變及行動
# CYBERSECURITY RESPONSE AND OPERATION

網絡安全事故應變
Cybersecurity Incident Response

主動網絡安全行動
Proactive Cybersecurity Operation

維護大型活動網絡安全
Safeguarding Cybersecurity in Major Events

# 網絡安全事故應變
# Cybersecurity Incident Response

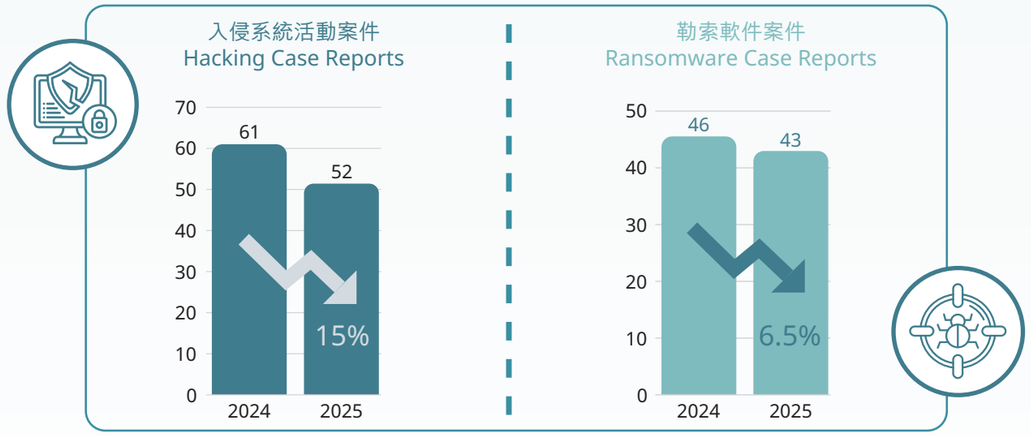
## 事故應變工作目的與核心價值
## Mission and Value of Incident Response

網罪科的網絡安全事故應變工作旨在支援本港不同機構處理網絡安全事故，目標是將損害降至最低、協助安全恢復營運，並透過成因分析與改善建議降低再次遭受攻擊的風險。我們的應變流程一般遵循五個階段：(一)初步研判與範圍界定、(二)封鎖與遏制、(三)根除威脅、(四)復原支援、(五)追溯根本成因及提出安全提升建議。

CSTCB's Incident Response (IR) function supports organisations across Hong Kong in managing cybersecurity incidents, aiming to minimise impact, safely restore operation, and reduce the risk of recurrence through root-cause analysis and improvement recommendations. Our IR process typically follows a five-phase lifecycle: (1) Identification and Scoping, (2) Containment, (3) Eradication, (4) Recovery Support, and (5) Root-cause Analysis and Security Enhancement Recommendations.


2025年，警方共接獲52宗入侵系統活動案件，按年下降15%，造成總損失達6 260萬港元。同年警方亦接獲43宗勒索軟件案件，按年下降6.5%，最高勒索金額達到1 000萬港元。香港由於中小企集中、高度依賴面向互聯網的服務，以及頻繁的跨境金融交易，使得本地機構持續成為攻擊目標。以下歸納2025年網罪科所處理個案的主要觀察、典型案例及實務建議，供各持份者參考。

In 2025, HKPF received 52 hacking case reports, representing a year-on-year decrease of 15%, causing a total loss of HK$62.6 million. Police received 43 ransomware case reports in the same year, representing a year-on-year decrease of 6.5%. The maximum amount of ransom demanded was HK$10 million. Hong Kong's concentration of SMEs, reliance on internet-facing services, and frequent cross-border financial transactions continued to make local organisations attractive targets. The following sections distil our key observations, illustrative case studies, and practical recommendations drawn from CSTCB's case handling in 2025 for stakeholders' reference.




2025年的事故顯示，攻擊者慣常透過暴露或保護不足的遠端存取服務取得初始存取權，包括VPN入口、RDP，以及AnyDesk、TeamViewer等遠端管理工具。邊緣裝置弱點、憑證暴力破解及釣魚電郵亦為常見入口。成功攻陷後，攻擊者會收集憑證、提升權限，再經RDP及SMB橫向移動，逐步接觸伺服器區、虛擬化平台及管理介面等高價值目標。

在勒索軟件個案中，攻擊者普遍在觸發加密前先破壞或癱瘓備份系統，包括名義上離線但實際仍可經網絡存取的儲存裝置。他們亦傾向延遲加密以提高勒索成功率。數據盜竊同樣在加密前日益普遍，形成「雙重勒索」模式，攻擊者亦常利用系統內建工具或雲端服務將惡意流量混入正常活動中。

Incidents in 2025 revealed that attackers consistently gained initial access through exposed or weakly protected remote access services, including VPN portals, RDP, and tools such as AnyDesk and TeamViewer. Edge device vulnerabilities, credential brute-forcing, and phishing emails were also common entry points. After a successful compromise, attackers harvested credentials, escalated privileges, and moved laterally via RDP and Server Message Block (SMB) to reach high-value targets such as server segments, virtualisation platforms, and management interfaces.

In ransomware cases specifically, attackers routinely destroyed or disabled backup systems before triggering encryption. This included storage devices that were nominally offline but still network-reachable. Attackers also tended to delay encryption to increase the likelihood of successful extortion. Data exfiltration before encryption ("double extortion") became increasingly common, with attackers frequently using built-in operating system tools or cloud services to disguise malicious traffic as normal activity.


在2025年的事故處理中，網罪科發現有不少案件無法查明起始原因或判斷其勒索軟件家族，常見原因包括受攻擊機構EDR覆蓋不全、VPN及RDP日誌保留期過短、缺乏集中化的審計日誌，以及日誌遭攻擊者篡改或清除。這些缺口不僅延長了攻擊的持續時間，並增加了復原的複雜性，更令後續調查與監管決策面臨重大困難。可視性不足本身已成為一種威脅倍增因素：若欠缺一致的審計實務，應變效率將大打折扣。

During our incident responses in 2025, CSTCB found that a number of cases could not be definitively attributed in terms of the initial cause of compromise or the ransomware family involved. Common causes included incomplete EDR coverage at affected organisations, short retention periods for VPN and RDP logs, absence of centralised audit logging, and log clearing or deletion. These gaps not only prolonged attack dwell time and complicated recovery, but also made subsequent investigation and regulatory decisions significantly more challenging. Insufficient visibility has become a threat multiplier in its own right: without consistent audit practices, response effectiveness is severely diminished.

2025年的個案中，多項反覆出現的結構性弱點令攻擊者有機可乘。在遠端存取層面，外露的RDP及VPN服務常配以弱密碼且缺乏多重認證，未獲授權的遠端工具則在欠缺集中管理的情況下運行。而邊界設備及韌體更新滯後，導致已知漏洞未能及時修補。在端點防護方面，資產清單不完整導致EDR覆蓋出現盲區，部分端點的授權甚至已經過期。

在應變與備份方面，雖然系統有發出安全警報，但卻缺乏明確的分流與事故升級機制，尤其是非辦公時間。另外，備份伺服器可從一般端點存取，缺乏不可變更或真正隔離的設計，令攻擊者得以將生產數據連同備份一併摧毀。此外，UAT等非生產環境因安全配置不足，亦成為入侵更敏感網絡的跳板。

Across cases in 2025, several recurring structural weaknesses enabled attackers. At the remote access layer, exposed RDP and VPN services were frequently paired with weak passwords and lacked multi-factor authentication, while unauthorised remote tools operated without central governance. Edge devices and firmware updates lagged behind, leaving known vulnerabilities unpatched. On the endpoint side, incomplete asset inventories resulted in EDR blind spots, with some endpoints operating on expired licences.

On the response and recovery side, security alerts were generated but lacked clear triage and incident escalation procedures, particularly outside business hours. Furthermore, backup servers remained reachable from standard endpoints and lacked immutable or truly isolated designs, allowing attackers to destroy backups alongside production data. Non-production environments such as UAT, often with weaker security controls, also served as stepping stones into more sensitive networks.

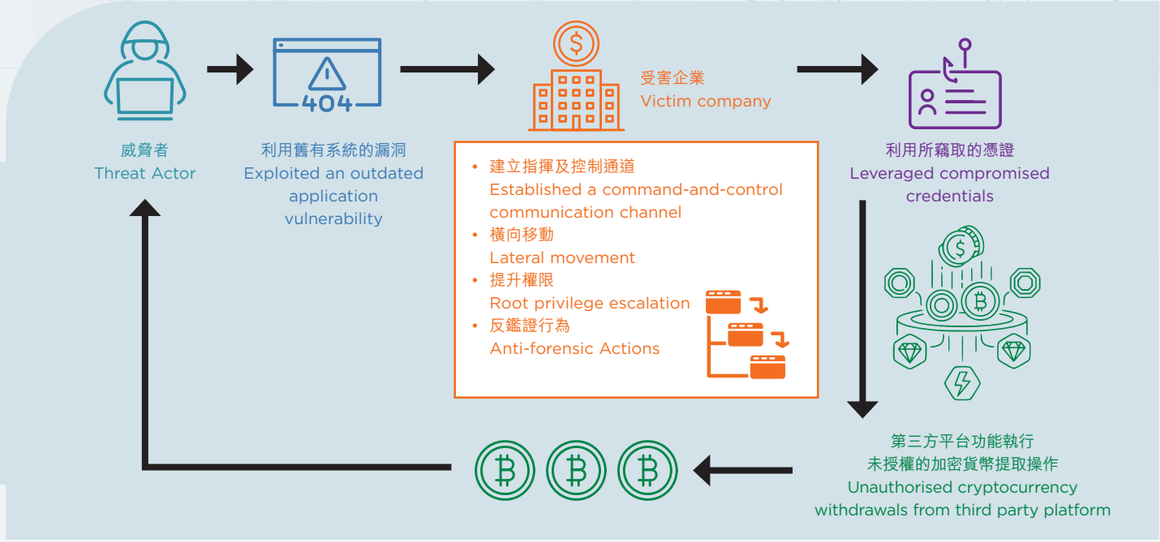
# 個案分享 Case Sharing

## 個案八 Case Study 8

### 多階段入侵導致資金損失
### Multi-stage cyber intrusion leading to financial theft

2025年，香港一間金融服務機構遭受多階段網絡入侵。攻擊者利用防護較弱的舊有系統作為初始入口，建立命令與控制通道並逐步進行橫向移動、提升權限，最終存取了高價值服務。其後，攻擊者採取反鑑證措施（例如清除日誌）以降低後續追查的可視性，繼而利用所竊取的憑證及第三方平台功能執行未授權的加密貨幣提取操作。

In 2025, a Hong Kong-based financial services organisation was subjected to a multi-stage cyber intrusion, which commenced with the exploitation of an outdated application in a less-protected environment. The attacker established command-and-control capabilities, proceeded with lateral movement, and escalated privileges to access high-value services. Subsequently, the attackers conducted anti-forensic actions (such as log clearing) to reduce visibility for later-stage investigation. Eventually, the attacker leveraged compromised credentials to access third-party platform functionalities and executed unauthorised cryptocurrency withdrawals.

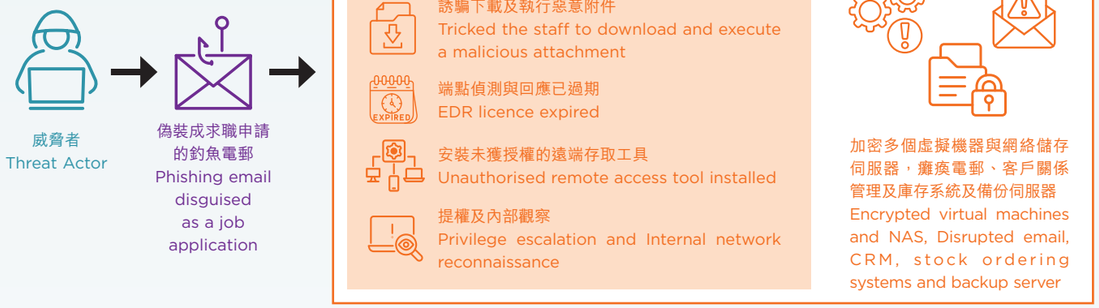



## 個案九 Case Study 9

### 針對香港餐飲集團的勒索軟件攻擊
### Ransomware attack against a Hong Kong restaurant group

2025 年 11 月，一個香港餐飲集團遭受RedCurl 團伙利用QWCrypt勒索軟件發動的攻擊。攻擊者以偽裝成求職申請的網絡釣魚電郵，誘使人力資源經理下載並執行惡意附件。該端點的EDR授權當時已過期，而且系統內安裝了未獲授權的遠端存取工具。攻擊者取得備份伺服器的管理員權限並潛伏約79天後，加密多個虛擬機器，癱瘓電郵、客戶關係管理及庫存系統，備份伺服器及異地NAS亦遭摧毀，所幸其POS系統因網絡分段而維持運作。值得注意的是，該機構在2024年已因缺乏多重認證的VPN帳號遭受勒索攻擊。事後改善僅針對VPN，未有全面處理電郵安全、備份設計及監控等結構性弱點，結果導致透過不同攻擊途徑再次受到入侵。

In November 2025, a Hong Kong restaurant group suffered a "QWCrypt" ransomware attack attributed to the RedCurl group. The attacker lured the HR manager into downloading and executing a malicious attachment via a phishing email disguised as a job application. The affected endpoint had an expired EDR licence and an unauthorised remote access tool installed. After obtaining administrative access to the backup server and dwelling for approximately 79 days, the attacker encrypted multiple virtual machines, crippling email, CRM, and inventory systems. Backup servers and offsite NAS were also destroyed. Fortunately, POS systems survived due to network segmentation. Notably, the same organisation had been hit by ransomware in 2024 via an MFA-less VPN account. Post-incident fixes addressed only the VPN, leaving structural weaknesses in email security, backup design, and monitoring unresolved, which allowed a successful attack through a different vector.




## 個案十 Case Study 10

### 針對公營機構網上服務的大規模短訊一次性密碼濫用
### Large-scale SMS OTP Abuse against a Public-Sector Online Service

2025年，有公營機構網上服務遭大規模濫用短訊一次性密碼功能，產生了巨額短訊費用。該服務的一次性密碼觸發介面可從客戶端組件中被發現，令攻擊者得以大規模發送自動化請求。儘管已部署驗證碼防護，攻擊者仍得以規避該措施，再次大量生成短訊。這類「低技術、高影響」的攻擊模式無需深度漏洞利用，卻足以造成直接財務損失及導致服務不穩定。此案例凸顯一次性密碼傳送所牽涉的供應鏈（驗證碼供應商、短訊閘道、應用程式供應商）需要清晰的共同責任劃分與迅速的集體應對機制。

In 2025, a public-sector organisation's online service suffered repeated large-scale abuse of its SMS OTP function, resulting in substantial SMS charges. The OTP triggering interface was discoverable from client-side components, enabling automated requests at scale. Although CAPTCHA was deployed, attackers were able to circumvent it and resumed bulk generation. This "low-sophistication, high-impact" pattern required no deep exploitation yet caused direct financial loss and service instability. The case highlights that OTP delivery depends on a supply chain (CAPTCHA providers, SMS gateways, application vendors) in which effective control requires clear shared responsibilities and rapid collective response.


## 主要啟示 Key Takeaways

綜觀2025年事故應變個案，可歸納出三項核心啟示。

Three core lessons emerge from the 2025 incident response caseload.

**1** 第一，初始入侵途徑高度集中於保護不足的遠端存取服務及邊緣裝置，反映攻擊面管理與身份驗證強化仍是防禦體系中最需優先處理的環節。

First, initial access remained heavily concentrated on poorly protected remote access services and edge devices, reflecting that attack surface management and identity hardening continue to be the most urgent priorities in the defence programme.

**2** 第二，備份架構的設計假設往往過於樂觀，多宗個案顯示備份憑證與生產環境共用同一集中式身份驗證系統，一旦該系統遭攻陷，備份即同時失守，令系統難以復原。

Second, backup architectures were frequently designed on overly optimistic assumptions. Multiple cases revealed that backup credentials shared the same centralised authentication infrastructure as the production environment, meaning that once that infrastructure was compromised, backups were lost simultaneously and recovery was hindered.

**3** 第三，可視性不足已成為影響調查成效的關鍵瓶頸。在多個勒索軟件個案中，因日誌覆蓋不全或遭清除，致使無法確認感染源頭或歸因其勒索軟件家族，不僅延長了攻擊者的潛伏時間，更嚴重妨礙事後調查。

Third, insufficient visibility has become a critical bottleneck for investigation effectiveness. In multiple ransomware cases, incomplete or cleared log coverage prevented definitive identification of the infection source or ransomware family attribution, prolonging attacker dwell time and severely hindering post-incident investigation.

上述啟示與本報告第3.4節「網絡安全建議」所提出的十項措施直接對應，相關建議涵蓋存取控制、備份韌性、日誌管理及事故應變準備等範疇，讀者可參閱該章節以獲取具體的操作性指引。

These lessons map directly to the ten cybersecurity mitigations presented in Section 3.4 of this report, which address access control, backup resilience, log management, and incident response preparedness among other areas. Readers are encouraged to refer to that chapter for detailed, actionable guidance.

# 主動網絡安全行動
# Proactive Cybersecurity Operation

## 「秒擊」淨網行動
## Cyber Hygiene Operation "INSTANTHIT"

為偵測及清除香港境內的惡意網絡基礎設施，網罪科於2025年1月至9月期間展開代號「秒擊」（INSTANTHIT）的淨網行動，聯同國際刑警、網絡安全特別行動小組的多家機構及多間本地和海外互聯網服務供應商，透過加強情報交流與合作，致力提升香港的網絡安全和韌性。

In order to detect and dismantle malicious cyber infrastructure in Hong Kong, CSTCB conducted a cyber hygiene operation codenamed "INSTANTHIT" between January and September 2025, in collaboration with INTERPOL, cybersecurity organisations of CSATF, and a number of local and overseas Internet Service Providers (ISPs). This joint initiative strengthened intelligence sharing and cooperation, aiming to enhance Hong Kong's overall cyber resilience.



在秒擊行動期間，網罪科成功偵測及清除了479台命令與控制伺服器、4 813部殭屍電腦，以及34 556個釣魚網站，並檢取超過1 500 GB數據進行數碼鑑證分析。行動所清理的命令與控制伺服器主要支援殭屍網絡操控、勒索軟件、釣魚詐騙、惡意程式傳播及資料竊取等攻擊。同時，互聯網服務供應商應網罪科要求，協助通知超過38萬部存有網絡安全風險的電腦及伺服器的用戶，提供實用指引以協助其及時修補相關漏洞。

During the INSTANTHIT operation, CSTCB detected and dismantled 479 C2 servers, 4,813 botnet-infected devices, and 34,556 phishing websites. More than 1,500 GB of data was collected for digital forensic analysis. The C2 servers dismantled in the operation were primarily used to support attacks involving botnet orchestration, ransomware deployment, phishing scams, malware distribution, and data exfiltration. Additionally, at CSTCB's request, ISPs notified the users of more than 380,000 computers and servers with cybersecurity risks and provided them with practical guidance to facilitate the timely remediation of the relevant vulnerabilities.

## 「RAPIDSTRIKE」行動
## Operation RAPIDSTRIKE

「RAPIDSTRIKE」行動是國際刑警組織與香港警務處於2025年7月攜手展開的一項重點網絡犯罪預防行動，旨在配合國際刑警 2022-2025 年全球戰略，全力打擊跨國網上詐騙及科技罪案。行動在國際刑警網絡犯罪專家組的框架下運作，核心目標是加強各成員國之間的情報交流與協作，以應對日益嚴峻的網絡威脅。其關鍵技術支援來自香港警務處於2025年4月在「守網聯盟」框架下開發的 AI 驅動系統「Project RAPID」。該系統能對可疑網站的域名特徵及網頁代碼進行即時、多維度分析，迅速識別新建立的惡意網站，從而精準鎖定相關伺服器位置，並即時通報成員國執法機構進行攔截或關閉，在騙案發生前實現主動阻截。

整項行動劃分為五個階段，包括每兩週一次的定期情報共享及行動結束後的全面評估。於2025年7月至2026年2月期間，已向超過35個成員國通報逾六千個可疑網站的資訊，以供調查及取締。行動不僅著眼於短期打擊，更致力深化及拓展調查範圍，以長遠瓦解犯罪網絡。透過實踐國際刑警網絡犯罪專家組的四大支柱（戰略、調查、預防及賦權），「RAPIDSTRIKE」行動將有效整合國際刑警組織成員國的資源，建立統一陣線，共同構建更具韌性的全球網絡安全環境。

Operation RAPIDSTRIKE is a strategic collaborative initiative between INTERPOL and the HKPF, launched in July 2025 to combat transnational online scams and technology crimes in alignment with INTERPOL's Global Cybercrime Strategy 2022-2025. Operating within the framework of the INTERPOL Cybercrime Expert Group (CyberEX), its core objective is to enhance intelligence exchange and cooperation among member countries against the growing cyber threat landscape. The operation is powered by Project RAPID, an AI-driven system developed by the HKPF in April 2025 under the "CyberDefender" framework, which performs real-time, multi-dimensional analysis of suspicious websites' domain characteristics and page code to rapidly identify newly created malicious sites. This intelligence enables Operation RAPIDSTRIKE to pinpoint associated hosting servers and promptly notify law enforcement agencies in member countries to block or take down these platforms, achieving proactive interdiction before scams are executed.

Structured into five phases, including bi-weekly intelligence-sharing sessions and a comprehensive post-operational assessment, the operation disseminated details of more than 6,000 suspicious websites to over 35 countries for investigations and takedowns between July 2025 and February 2026. Beyond short-term disruption, it also seeks to deepen and broaden investigations with the long-term objective of dismantling criminal networks. By operationalising CyberEX's four pillars — Strategy, Investigation, Prevention, and Empowerment — Operation RAPIDSTRIKE integrates resources from INTERPOL member countries to establish a unified front and collectively build a more resilient global cybersecurity landscape.

## 檢控案件分享
## Prosecution Case Sharing

### 智鬥行動（深偽技術相關的詐騙案件）
### Operation WITSGAME (Deepfake related Fraud)

於2025年2月，網罪科接獲數字銀行報告，指多宗網上開戶申請中，申請人的即時自拍與身份證照片不符。調查發現，一個本地詐騙集團於2024年3月至2025年2月期間，盜用已報失的香港身份證，透過篡改身份證影像及深偽換臉技術配合即時自拍，成功通過驗證，開設30個銀行帳戶，進行貸款申請及信用卡消費，造成86萬港元損失，並清洗逾120萬港元犯罪得益。

2025年4月，網罪科以涉嫌「串謀詐騙」及「處理已知道或相信為代表從可公訴罪行的得益的財產」（俗稱洗黑錢）等罪名拘捕9人，包括主腦及骨幹成員。並在檢獲的電子設備中發現用於生成深偽頭像的手機應用程式。是次行動有賴警方與數字銀行緊密合作，並促使業界強化數碼身份驗證程序。

In February 2025, several digital banks reported to CSTCB that applicants' live selfies did not match their HKID photos during online account applications. Investigation revealed that a local fraud syndicate, operating between March 2024 and February 2025, had exploited lost HKID cards with tampered images and deepfake face-swapping, combined with live selfies to bypass verification. The syndicate successfully opened 30 accounts for loan applications and credit card purchases, causing losses of HK$860,000 and laundering over HK$1.2 million in crime proceeds.

In April 2025, CSTCB arrested nine individuals including the mastermind and core members for offences of "Conspiracy to Defraud" and "Dealing with Property Known or Believed to Represent Proceeds of an Indictable Offence" (commonly known as money laundering), with digital forensic examination of seized devices uncovering the mobile application used to generate the deepfake portraits. The operation was enabled by close collaboration between the HKPF and digital banks, prompting the industry to enhance its digital identity verification processes.

## 檢控案件分享
## Prosecution Case Sharing

### 謀攻行動 (詐騙、科技罪案及相關洗黑錢案件)
### Operation ATTACKPLAN (Fraud, Technology Crime and related Money Laundering cases)

於2025年4月及8月，刑事部聯同各大總區展開兩次全港性執法行動，代號為「謀攻」，以打擊詐騙、科技罪案及相關洗黑錢罪行。

在這兩次行動中，一共拘捕863名人士，涉嫌「串謀詐騙」、「以欺騙手段取得財產」及「處理已知道或相信為代表可公訴罪行得益的財產」(俗稱洗黑錢)等罪行。相關案件涉及733宗詐騙案及科技罪案，涉款總額超過19億港元。

於2025年8月的行動中，網罪科成功瓦解一個利用網上社交平台發布偷拍相片及淫褻物品的本地犯罪集團。經調查後，網罪科發現該集團在社交平台設立一個免費公開頻道，並於頻道內發布各類色情主題的預覽影片及相片，以招攬會員繳付一次性會費，加入私人頻道以瀏覽所有內容。相關內容除涉及淫褻不雅物品外，亦包括學生裙底偷拍影片及相片。

In April and August 2025, Crime Wing, in collaboration with other Regions, mounted two territory-wide enforcement operations codenamed "ATTACKPLAN", combating fraud, technology crime and related money laundering cases.

In the two operations, a total of 863 individuals were arrested for offences including "Conspiracy to Defraud", "Obtaining Property by Deception", and "Dealing with Property Known or Believed to Represent Proceeds of an Indictable Offence" (commonly known as money laundering). The arrests were in connection with 733 fraud and technology crime cases, involving total losses of over HK$1.9 billion.

In the enforcement operation carried out in August 2025, CSTCB successfully dismantled a local crime syndicate that exploited a social media platform to distribute surreptitiously taken photos and obscene materials. Upon investigation, CSTCB discovered that the syndicate had set up a free public channel on a social platform, where preview videos and images of various pornographic themes were posted to attract members. Interested individuals were solicited to pay a one-off membership fee to gain access to a private channel containing all content. The materials included not only obscene and indecent items but also upskirt videos and photos of students.



調查顯示，該頻道由兩名集團主腦操控，其餘骨幹成員則負責提供色情及偷拍影像，交由主腦在頻道上發布。涉事偷拍影像全部以女性為目標，大部分拍攝於本地公共交通工具、車站及商場等人流密集地點。兩名主腦利用多個屬於家人及集團成員的銀行帳戶及支付工具戶口，收取並清洗透過營運上述頻道所得的犯罪收益，涉款逾400萬港元。

網罪科於行動中以「串謀在未經同意下發布私密影像」、「串謀發布淫褻物品」以及「洗黑錢」等罪名共拘捕11人，包括兩名集團主腦及懷疑負責提供相片的偷拍成員，並於被捕人家中檢獲與案件相關的重要證據。在拘捕行動後，警方已將相關社交平台的頻道封鎖。網罪科會繼續以情報主導的方式，與各持份者合作，全力打擊網上罪案。

Investigation revealed that the channel was operated by two masterminds of the syndicate, while other core members were responsible for supplying pornographic and surreptitiously taken images for publication. All of the surreptitious recordings targeted women, and were mostly captured in local public transport, stations, shopping malls, and other crowded venues. The two masterminds used multiple bank accounts and stored value facility accounts belonging to family members and syndicate associates to collect and launder the criminal proceeds generated from the channel operation, with the amounts laundered exceeding HK$4 million.

During the operation, CSTCB arrested 11 individuals for the offences of "Conspiracy to Publish Obscene Articles", "Conspiracy to Publish Intimate Images without Consent", and "Money Laundering", including two masterminds and core members suspected of providing the surreptitiously taken images. Crucial evidence related to the case was seized from the residences of the arrested persons. Following the arrests, the Police blocked the relevant social media channel. CSTCB will continue to adopt an intelligence-led approach and work closely with our stakeholders to combat technology crime.

### 利用「偽基站」發送釣魚短訊
### Utilisation of Pseudo Base Station for Sending Phishing SMS

2023年12月，通訊事務管理局辦公室(通訊辦)實施「短訊發送人登記制」。根據此制度，已登記的單位在發送短訊予本地流動電話用戶時，發送人名稱前方會加上「#」號，以供識別發送人身份。

2025年2月，警方接獲公眾舉報，指有市民收到帶有上述(#)號、偽冒政府部門、物流公司及電子支付平台的詐騙短訊，內容附有釣魚連結，誘使市民輸入信用卡資料。

網罪科隨即聯同通訊辦及流動網絡營辦商跟進事件，並追查所有收到相關短訊地點的閉路電視錄像。經深入調查後發現，不法份子以車輛運載「偽基站」流竄全港各區，利用「偽基站」干擾附近公眾的手機訊號及發送偽冒短訊。

In December 2023, the Office of the Communications Authority (OFCA) launched the "SMS Sender Registration Scheme". Under this scheme, when verified entities send SMS to local mobile users, their sender names are prefixed with the '#' prefix to facilitate sender identification.

In February 2025, police received reports from the public that individuals received phishing SMS bearing the prefix '#' and purportedly to be from registered government departments, logistic companies and e-payment platforms, containing phishing links designed to lure victims into entering their credit card information.

CSTCB promptly collaborated with OFCA and Mobile Network Operators to investigate the incident, including reviewing CCTV footage from all locations where such SMS were received. The subsequent in-depth investigation revealed that the culprits had used vehicles to transport a Pseudo Base Station across various areas in Hong Kong, employing the Pseudo Base Station to interfere with the public's mobile signals and send phishing SMS.


2025年2月17日，網罪科人員截查一輛可疑客貨車，在車上拘捕一名男子。現場檢驗證實，該名男子利用其手機應用程式編寫帶有上述「#」號的偽冒短訊，然後經車內的「偽基站」發送至附近的手機用戶。

2025年12月，該名男子在東區裁判法院被裁定「串謀詐騙」及「無牌管有無線電通訊器具」兩項罪名成立，分別判處監禁十五個月及兩個月。此案是香港首宗涉及使用偽基站進行詐騙並成功定罪的案件。在此案之後，網罪科主動與監管機構及業界分享案例及技術關注點，並研究主動偵測、防範及通報機制，以協作方式共同維護本港電訊環境的安全。

On 2025-02-17, CSTCB officers intercepted a suspicious light goods vehicle and arrested a man inside. Examination at the scene confirmed that the man had used a mobile application to compose phishing SMS with '#' prefix, which were then transmitted to nearby mobile users via the Pseudo Base Station installed in the vehicle.

In December 2025, the defendant was convicted of the offences of "Conspiracy to Defraud" and "Possession of apparatus for telecommunications without a licence" at the Eastern Magistrates' Court, and was sentenced to 15 months' and 2 months' imprisonment respectively. This case marked Hong Kong's first successful prosecution involving the use of a Pseudo Base Station for fraudulent activities. In this case, CSTCB proactively shared the case details and relevant technical concerns with regulators and industry stakeholders, and explored proactive detection, prevention and reporting mechanisms to collaboratively safeguard the security of Hong Kong's telecommunications environment.

# 維護大型活動網絡安全
# Safeguarding Cybersecurity in Major Events

## 大型活動網絡安全準備與協調工作
## Major Event Cybersecurity Preparedness and Coordination

香港警務處在制訂大型活動安保方案時，網罪科負責擔任網絡安全行動的主導角色，與政府部門、主辦機構及其他公私營持份者緊密合作。2025年，「第十五屆全國運動會」(全運會)及「第八屆立法會換屆選舉」是本港兩項重要活動。網罪科在籌備及執行階段與各持份者緊密協作，確保活動最終圓滿完成，達成了網絡安全零事故的目標。

When the HKPF formulates operational plans for major events, CSTCB serves as the Cybersecurity Operation Lead, working closely with government departments, organisers, and other public and private sector stakeholders. In 2025, the 15th National Games (NG) and the 8th Legislative Council General Election (LCGE) were two major events in Hong Kong. CSTCB worked in close collaboration with stakeholders throughout the preparation and execution phases to ensure these events concluded successfully and achieved the goal of zero cybersecurity incidents.

## 風險評估 Risk Assessment

網罪科積極與各持份者協作，並於大型活動舉行前及期間提供一系列網絡安全防護措施，以保障其關鍵資訊科技系統免受潛在網絡攻擊。此外，網罪科亦進行了實地巡查，走訪場館及票站，旨在評估各處所的資訊安全狀況。巡查期間，網罪科向持份者提供了改善建議，包括加強網絡邊界防禦、縮小攻擊面，以及確保網絡得到妥善分隔。

CSTCB actively collaborated with stakeholders, providing a series of cybersecurity protection measures before and during major events to safeguard their critical IT systems against potential cyberattacks. Furthermore, CSTCB conducted on-site visits to venues and polling stations to assess the information security posture of each location. During these inspections, recommendations were given to stakeholders to enhance on-site cyber defences, reduce the attack surface, and ensure proper network segregation.

## 網絡威脅情報共享
## Threat Intelligence Sharing

在立法會換屆選舉和第十五屆全運會舉行之前，網罪科持續與本地及國際網絡安全機構合作，交換並分享網絡威脅情報，協助相關持份者加強防禦並及時採取應對措施，以全面提升防護能力。同時，網罪科展開「淨網行動」，針對活動相關的命令與控制伺服器及可疑域名進行主動偵測與下架，以減少潛在攻擊風險。此外，在重大活動前後，網罪科亦會加強網絡巡邏，並與持份者保持緊密聯繫，確保防護措施切實執行，從而保障活動順利舉行。

Prior to the LCGE and the 15th NG, CSTCB strengthened collaboration with local and international cybersecurity agencies to exchange and share threat intelligence, enabling stakeholders to enhance defensive measures and take timely response actions to mitigate potential cyber risks. CSTCB also launched Cyber Hygiene Operation to proactively detect and take down event-related C2 servers and suspicious domain names, thereby reducing potential attack vectors. In addition, cyber patrols were intensified before, during and after the events, with close liaison maintained with relevant stakeholders to ensure protective measures were effectively implemented and that the events were conducted in a safe and orderly manner.

## 演習與演練 Exercise and Drills

為迎接第十五屆全運會及確保啟德體育園的順利啟用，網罪科籌劃並參與了多項桌上演練，使持份者深入掌握不同網絡攻擊的潛在影響及相關應對流程。

In preparation for the 15th NG and to ensure the smooth opening of the Kai Tak Sports Park, CSTCB planned and took part in various tabletop exercises and drills, enabling stakeholders to gain a thorough understanding of the potential impacts of different cyberattacks and the corresponding response process.

2025年9月9日，網罪科於警察總部舉辦了代號為「舉劍者」的網絡安全研討會暨桌上演練。活動吸引超過30個部門、機構及組織逾百多名代表參與，參與者包括全國運動會香港賽區統籌辦公室、場館營運商、多個政府部門、運輸及公共機構，以及相關體育總會。是次活動圓滿舉行，充分彰顯了跨界別協作的關鍵作用。

On 9 September 2025, CSTCB conducted the Cyber Security Seminar cum Tabletop Exercise, codenamed SWORDLIFTER, at the Police Headquarters. The event attracted over 100 representatives from more than 30 departments, agencies and organisations, including the National Games Coordination Office (Hong Kong), venue operators, various government departments, transportation and public organisations, as well as relevant sports associations. The event concluded successfully, strongly demonstrating the critical role of cross-sector collaboration.

為確保立法會選舉順利進行，網罪科於2025年第三及第四季度與選舉事務處及數字政策辦公室共同開展了兩次桌上演習。這些演習旨在完善應對網絡安全事故的通訊協定及協調機制，並測試相關應變流程及後備方案的運作效能。

To ensure the smooth conduct of the Legislative Council Election, CSTCB jointly conducted two tabletop exercises with the Registration and Electoral Office and the DPO in the 3rd and 4th quarters of 2025. These exercises aimed to enhance communication protocols and coordination mechanisms for managing potential cybersecurity incidents, as well as to test the effectiveness of relevant response procedures and fallback arrangements.

## 網絡安全測試 Cybersecurity Tests

網罪科於大型活動舉行前進行全面網絡安全測試，主動識別持份者系統中的潛在漏洞。一經發現相關漏洞，網罪科隨即指示持份者立即進行修復或予以消除。此項預防措施旨在提升持份者的安全防護能力，從而降低大型活動期間遭受網絡攻擊的風險。

CSTCB conducted comprehensive cybersecurity testing prior to major events to proactively identify vulnerabilities within stakeholders' systems. Upon discovery of these vulnerabilities, CSTCB directed the stakeholders to promptly remediate or eliminate them. This preventive measure was designed to enhance stakeholders' security posture and reduce the risk of cyberattacks during the events.

## 事故應變 Incident Response

在大型活動舉行期間，網罪科建立了穩健的實時監察機制。除了營運內部網絡安全中心外，網罪科亦調派相關人員至活動專責的網絡指揮中心，於活動期間監察關鍵系統的安全及運作狀況。同時，網罪科派遣人員駐守各個場館，以提供即時事故應變支援，並在有需要時於現場進行數碼法理鑑證分析。

During major events, CSTCB implemented a robust real-time monitoring mechanism. In addition to operating its internal Cyber Security Centre, CSTCB deployed personnel to the event-specific cybersecurity command centre throughout the event period to monitor the security and operational status of critical systems. CSTCB also stationed officers at various venues to provide on-site incident response support and to conduct immediate digital forensic analysis when required.

# 活動圓滿結束
# Successful Conclusion of the Events

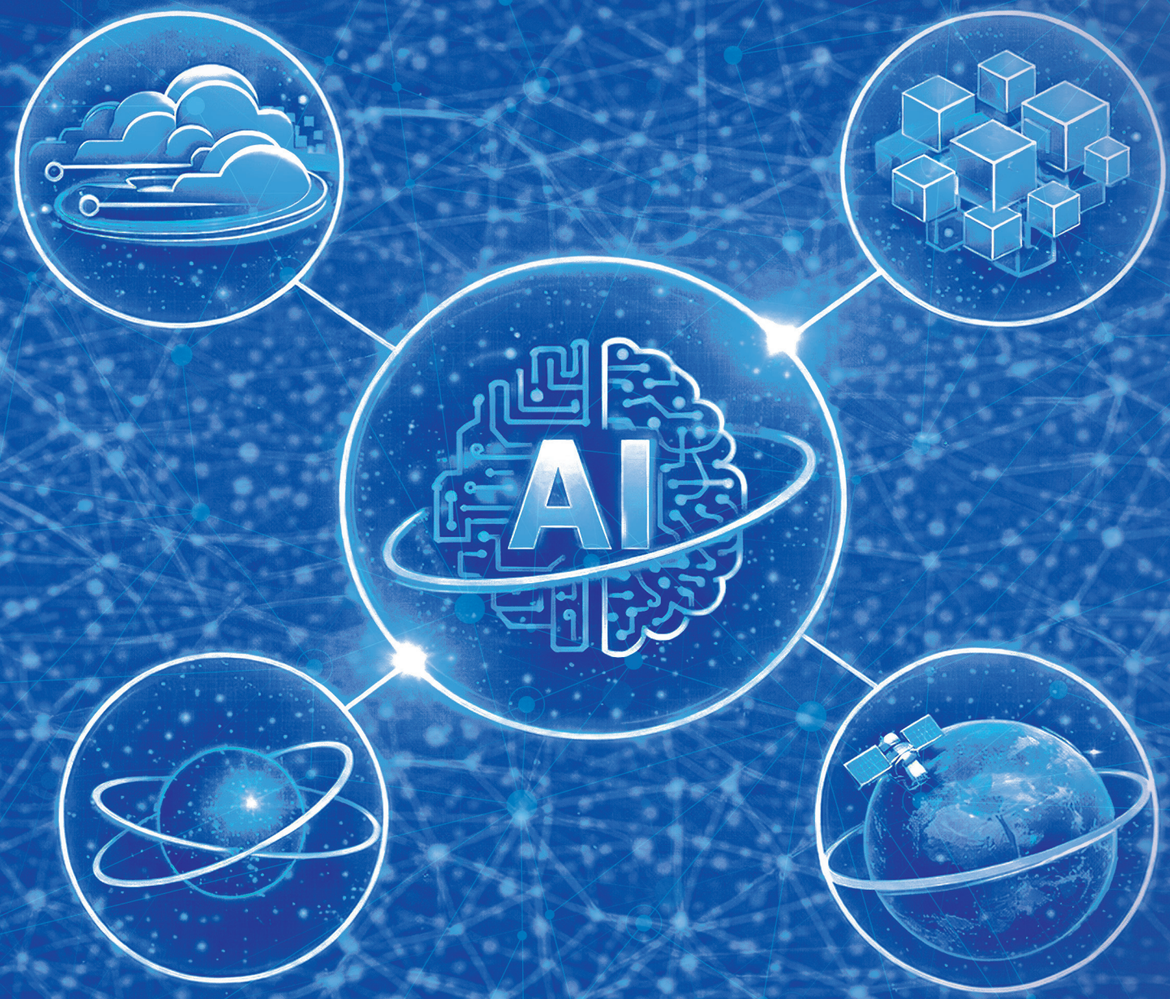
網罪科深感榮幸能參與並承擔相關大型活動的網絡安保工作。憑藉成功強化網絡防禦能力，網罪科協助確保各項活動得以在安全、有序且無任何網絡安全事故的環境下圓滿結束。

CSTCB is honoured to have participated in and undertaken the cybersecurity responsibilities for these major events. By successfully enhancing cybersecurity defences, CSTCB helped ensure that the events were conducted in a safe, orderly, and secure manner, with no cybersecurity incidents.

展望未來，網罪科將繼續致力提升社會各界對網絡安全的認知，並加強整體網絡防禦能力，為未來的大型活動作好充分準備。網罪科深知跨部門協作的重要性，定必積極推動業界最佳實踐、擴展網絡安全演練的參與範圍，並推進各項防禦措施，以提升整體應變水平。此外，網罪科將透過深化持份者協作，並把網絡安全元素全面納入規劃及運作流程，全力構建一個防禦穩健的生態系統，讓各持份者明確自身職責，攜手協力保障未來大型活動的安全。

Moving forward, CSTCB will continue to strive towards enhancing cybersecurity awareness and reinforcing defensive capabilities across all sectors of society, ensuring full preparedness for future major events. Recognising the vital role of cross-agency collaboration, CSTCB is committed to promoting industry best practices, broadening participation in cybersecurity exercises, and advancing defensive measures to elevate overall response capabilities. Furthermore, by deepening stakeholder engagement and embedding cybersecurity considerations fully into planning and operational processes, CSTCB aims to build a robust defensive ecosystem in which all stakeholders clearly understand their responsibilities and work together to safeguard future major events.

# 網絡威脅預測 2026+
CYBER THREAT FORECAST




量子技術 Quantum

區塊鏈 Blockchain

雲端運算 Cloud Computing

衛星技術 Satellite

人工智能 Artificial Intelligence

## 量子技術 Quantum

量子通訊安全 Quantum Communication Security

量子運算威脅 Quantum Computing Threats

去中心化金融 Decentralised Finance (DeFi)

在香港推動「智慧城市」及「低空經濟」的過程中，數碼基建與金融科技持續發展，網絡安全風險亦相應增加。目前，量子技術尚未普及，但其潛在威脅在於未來可能破解現有加密標準。業界已開始研究後量子密碼學，以應對未來加密標準可能面臨的挑戰。

In the process of promoting "Smart City" and the "Low-Altitude Economy" in Hong Kong, the continuous development of digital infrastructure and financial technology has also led to a corresponding rise in cybersecurity risks. Although quantum technology is not yet accessible to all, its potential threat lies in the possibility that it could one day break current encryption standards. The industry has begun researching post-quantum cryptography to address the challenges that future encryption standards may face.

## 區塊鏈 Blockchain

去中心化身份 Decentralised Identity (DID)

智能合約漏洞 Smart Contract Vulnerabilities

合規風險 Compliance Risks

加密貨幣 Cryptocurrency

香港《穩定幣條例》於2025年8月生效，為虛擬資產監管奠定重要基礎。隨著區塊鏈在金融及跨境支付中普及，智能合約漏洞、跨鏈橋攻擊及去中心化交易所（DEX）安全風險等技術性威脅值得關注。在現有監管基礎上持續完善技術保障，將鞏固香港作為安全創新的虛擬資產中心地位。

Hong Kong's Stablecoins Ordinance, effective since August 2025, marks a significant step in regulating virtual assets. As blockchain adoption grows in financial services and cross-border payments, emerging challenges warrant attention. Smart contract vulnerabilities, cross-chain bridge exploits, and the nature of Decentralised Exchanges (DEXs) present evolving cyber risks. Building on the current regulatory foundation, further measures addressing these technical dimensions would strengthen Hong Kong's position as a secure and innovative virtual asset hub.

## 雲端運算 Cloud Computing

設定錯誤與共用責任風險 Misconfiguration and Shared Responsibility Risks

資料隱私與保護 Data Privacy and Protection

雲端運算方面，數字政策辦公室已發布《雲端運算保安實務指引》，為企業數據保護提供重要指導。隨著多雲及混合雲架構日益普及，數據私隱保障成為關鍵議題，跨境數據傳輸及多租戶環境下的數據隔離風險尤需關注。此外，雲端服務的共享責任模式下，企業與供應商之間的安全責任劃分容易產生灰色地帶，導致配置錯誤及存取權限管理不當。在現有指引基礎上，進一步釐清共享責任並加強配置管理，將有助企業更安全地運用雲端服務。

For cloud computing, the DPO's "Practice Guide for Cloud Computing Security" provides important guidance for enterprise data protection. As multi-cloud and hybrid cloud architectures become more prevalent, data privacy concerns grow, particularly around cross-border data transfers and data isolation in multi-tenant environments. The shared responsibility model between cloud providers and enterprises can also create ambiguity in security obligations, leading to misconfigurations and inadequate access controls. Building on the existing guidance, further clarifying shared responsibilities and strengthening configuration management practices will help enterprises adopt cloud services more securely and confidently.

## 衛星技術 Satellite

香港已在監管沙盒中測試衛星導航干擾預警等安全技術，為低空經濟發展奠定基礎。隨著無人機應用規模擴大，訊號欺騙與干擾、無人機通訊鏈路安全及空域系統防護等挑戰將日趨顯著。持續完善相關保安標準，將有助低空經濟安全有序發展。

Hong Kong has tested satellite navigation interference warning systems within a regulatory sandbox, laying a foundation for the low-altitude economy. As drone applications scale up, challenges around signal spoofing and jamming, communication link security, and airspace system protection will become more prominent. Continued development of relevant security standards will support the safe and orderly growth of the low-altitude economy.

衛星通訊安全 Satellite Communication Security

資料完整性與加密 Data Integrity and Encryption

空域系統防護 Airspace system protection

香港在政策層面正逐步完善相關監管框架，包括於2026年實施《保護關鍵基礎設施（電腦系統）條例》，為關鍵基礎設施保護其系統安全建立基準要求，並透過持續的技術創新與跨境協作，在數碼化進程中平衡科技發展與網絡安全。

At the policy level, Hong Kong is progressively improving its regulatory frameworks. In 2026, the Protection of Critical Infrastructures (Computer Systems) Ordinance came into effect, establishing the baseline requirement to protect system security of critical infrastructures. Through ongoing technological innovation and cross-border collaboration, Hong Kong aims to balance technological advancement and cybersecurity in its digital transformation journey.

## 人工智能 Artificial Intelligence

AI驅動攻擊自動化 AI-Driven Attack Automation

資料隱私威脅 Data Privacy Threat

深偽技術 Deepfakes

演算法偏差安全 Algorithmic Bias Safety

惡意操控威脅 Malicious Manipulation Threat

除了深度偽造、社交操縱及自動化攻擊等新型威脅外，隨着愈來愈多AI工具可於個人設備上運行並與日常應用整合，用戶應核實AI的輸出結果，審慎授予敏感資料及系統權限，並了解自身資料的儲存及使用方式。對此，私隱專員公署已發布《開發及使用人工智能道德標準指引》及《人工智能：個人資料保障模範框架》，為機構應對相關挑戰提供實務指引。

Apart from emerging threats such as deepfakes, social manipulation and automated attacks, as AI tools increasingly operate on personal devices and integrate with everyday applications, users should verify AI-generated outputs, exercise caution when granting access to sensitive data and systems, and understand how their information is stored and used. The PCPD has issued "The Guidance on the Ethical Development and Use of Artificial Intelligence" and "The Artificial Intelligence: Model Personal Data Protection Framework" to provide practical guidance for organisations in addressing these challenges.

Mr. Neal JETTON

國際刑警組織網絡犯罪主管
Director of Cybercrime, INTERPOL

INTERPOL

網絡犯罪分子利用瞬息萬變的跨境關係、各國調查資源與能力參差不齊，以及執法部門之間即時資訊共享的延遲，最終對受害者造成傷害。隨著網絡威脅格局不斷擴大和演變，犯罪分子開始運用新興技術提升犯罪活動的效率和規模，全球執法機關建立「一體同心」的協作理念至關重要。國際刑警組織深知這些挑戰，並致力與香港警務處等緊密合作夥伴攜手，構築堅定不移的防線。我衷心感謝香港警務處的專業協作與貢獻，讓我們能更有效地共同打擊跨國網絡犯罪。

Cybercriminals exploit ever-changing cross-border relationships, disparate investigative resources and capabilities and delays in real-time information sharing between law enforcement to achieve success in harming their victims. As the cyberthreat landscape continues to expand and evolve, and emerging technologies are used by criminals to improve efficiency and scale of their acts, it is critical that global law enforcement develop a “one team” mentality.  INTERPOL recognises these challenges and is committed to working with its dedicated partners such as the HKPF to achieve steadfast resistance. I am grateful for HKPF’s partnership and expertise as together we combat transnational cybercrime more effectively.

快速發展的前沿科技與越趨複雜的供應鏈，正為網絡安全防禦技能帶來新挑戰。網絡安全專業人員正加速提升技術能力，與科技發展並肩前行，共同構築更強韌的防護體系。因此，政府、業界和學界必須攜手合作應對新興威脅，並積極培養網路安全人才，進而強化網路安全生態圈，將網絡安全積極融入數字轉型的各個階段，確保科技持續成為推動數字經濟發展的動力，而非風險之源。

The rapid development of cutting-edge technologies and increasingly complex supply chains are bringing new challenges to cybersecurity defence skills. Cybersecurity professionals are accelerating the enhancement of their technical capabilities, keeping pace with technological advancements to jointly build a more resilient protection system. Therefore, governments, industries and academia must work together to address emerging threats and actively nurture cybersecurity talent, fortifying the ecosystem. Cybersecurity must be actively integrated into each stage of digital transformation, ensuring that technology remains a driving force for advancement in the digital economy, rather than a source of risk.

張宜偉先生, JP
Mr. CHEUNG Yee Wai, Daniel, JP

現任署理數字政策專員
the incumbent Commissioner for Digital Policy (Acting)

中華人民共和國香港特別行政區政府
數字政策辦公室
Digital Policy Office
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

陳永安先生
Mr. Francis CHAN Wing-on

關鍵基礎設施（電腦系統安全）專員
Commissioner of Critical Infrastructure (Computer- system Security)

中華人民共和國香港特別行政區政府
保安局關鍵基礎設施（電腦系統安全）專員辦公室
Office of the Commissioner of Critical Infrastructure (Computer-system Security), Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

自2026年起，香港的關鍵基礎設施電腦系統安全由「認知」走向「實踐」。《保護關鍵基礎設施(電腦系統)條例》訂明營運者的責任，《實務守則》把要求轉化為可落實、可驗證的基線標準。真正的韌性不止於「紙上談兵」：它始於建立企業管治文化，並透過持續提升人員、流程與科技以落實安全要求，進一步延伸至供應商與合作夥伴。電腦系統安全不再只是資訊科技部門的事，而是關乎企業管治，並有賴公私營合作。

From 2026, Hong Kong’s computer-system security for critical infrastructures shifts from awareness to action.  The Protection of Critical Infrastructures (Computer Systems) Ordinance sets clear obligations for operators, and the Code of Practice translates these into an actionable baseline that can be implemented and evidenced.  True resilience goes beyond paper - it starts with establishing corporate governance culture, implementing security requirements through continuous improvement of people, process, and technology, and further extends to suppliers and partners.  Computer-system security is no longer only an IT matter, it is about corporate governance and relies on public-private partnership.



畢堅文先生, MH
Mr. Mohamed BUTT, MH

香港生產力促進局總裁
Executive Director, Hong Kong Productivity Council (HKPC)

hkpc 生產力局

根據香港網絡安全事故協調中心發布的《網絡安全展望2026》，2025年本港錄得15,877宗網安事故，按年上升27%，創下歷年新高；其中，人工智能相關攻擊與供應鏈漏洞已成為當前的頭號風險。面對日趨自動化的網絡攻擊，網絡安全創新的重心必須轉向人工智能管治、具風險意識的技術應用，以及人工智能驅動的防禦能力。為協助企業強化數碼韌性，香港網絡安全事故協調中心聯同數字政策辦公室推出「網絡安全服務供應商聯動計劃」，在四大關鍵服務範疇中網羅了 21家合資格的供應商，旨在共同構建更安全的數碼營商環境。

HKCERT’s Cybersecurity Outlook 2026 reveals that reported security incidents hit a record high of 15 877 in 2025, representing a 27% annual increase, with AI related attacks and supply chain vulnerabilities among the top risks. As cyberattacks become increasingly automated, cybersecurity innovation must prioritise AI governance, risk aware technology adoption, and AI enabled defensive capabilities. To help enterprises strengthen resilience, HKCERT partnered with the Digital Policy Office to launch the Cybersecurity Service Providers Connect Programme, bringing together 21 qualified providers across four key service areas. The initiative is to support a safer digital business environment.

隨著網絡攻擊愈趨複雜，企業必須採用零信任架構，從網站安全到企業內部系統全面加強，並提升員工及管理層的網絡安全意識，更須落實「系統、政策、人員」三重防護，推行多重驗證、定期漏洞檢測及數據加密，確保業務持續安全，降低風險，保障長遠發展。

With escalating cyberattacks, organisations need a Zero Trust framework to secure both external and internal environments. Beyond technology, fostering security awareness among employees and leadership is essential. A three-layered approach with systems, policies, and people which combined with MFA, regular vulnerability assessments, and encryption will strengthen resilience, reduce exposure, and safeguard sustainable growth.

黃家偉工程師
Ir Wilson WONG

香港互聯網
註冊管理有限公司行政總裁
CEO, Hong Kong Internet Registration Corporation Limited (HKIRC)

hkirc

鄭松岩博士
Dr. Rocky CHENG

數碼港行政總裁
CEO, Cyberport

數碼港 Cyberport

香港警方非常注重科技的應用，與時俱進地研究和引入最新技術的應用，例如人工智能、具身智能、數字技術等，以更好地維護社會和民眾的安全，同時舉辦不同活動以提升民眾和企業的網絡安全意識，令人欣慰。

網絡安全人人有責。政府、企業、民眾攜手合作，完善政策和標準、落實措施和演練、培養人才和意識，才能最大程度的防禦和抵擋日新月異的網絡攻擊，維護社會穩定和保護民眾生命財產的安全。

The Hong Kong Police Force places significant emphasis on the application of technology, keeping pace with the times by actively exploring and deploying cutting-edge innovations—such as artificial intelligence (AI), embodied AI, and digital technologies—to better safeguard society and the public. Furthermore, their efforts to organise various initiatives aimed at enhancing cybersecurity awareness among citizens and enterprises are highly commendable.

Cybersecurity is a collective responsibility that demands a unified front from the government, enterprises, and the public. By collaborating to refine policies and standards, execute rigorous measures and drills, cultivate talent and foster awareness, we can effectively mitigate the ever-changing cyberattacks, thereby maintaining social stability and protecting the lives and property of citizens.

顧榮輝教授
Professor GU Ronghui
CertiK聯合創辦人
Co-founder, CertiK

隨著數碼技術持續發展，網絡安全已從原本偏重技術層面的課題，演變為組織與社會韌性的核心要素。自動化、人工智慧以及數位服務的廣泛應用，正不斷重塑風險格局。這些日益複雜的威脅不僅衝擊系統，更影響人類決策流程，僅在2025年就導致業界損失超過33億美元。

應對這類挑戰需要採取均衡策略，結合有效治理、明確責任劃分，以及持久的公私營協作。持續重視網絡衛生、安全意識與應變準備，對於強化信任基礎、保障數位發展的長期穩健，依然至關重要。

As digital technologies continue to advance, cybersecurity has evolved from a predominantly technical concern into a core component of organisational and societal resilience. Automation, AI, and the expanding use of digital services continue to reshape risk profiles. These evolving threats now extend across systems as well as human decision-making and cost the industry over US$3.3B in 2025.

Addressing such challenges calls for a balanced approach, combining effective governance, clearly defined responsibilities, with sustained collaboration between public and private stakeholders. Continued emphasis on cyber-hygiene, awareness, and preparedness remains fundamental to strengthening confidence while safeguarding long-term digital growth.

當前，人工智能與區塊鏈賦能數字經濟的同時，卻也讓網絡犯罪趨於國際化、自動化、規模化和隱蔽化。超過80%的新型網絡犯罪涉及虛擬資產，同時AI生成仿真釣魚、偽造KYC與音訊視頻詐騙，為傳統安全防禦體系帶來新的挑戰。

楊霞教授
Professor YANG Xia
Beosin創辦人
Founder, Beosin

在Beosin，我們堅持創新，率先結合AI與大模型研發了先進的區塊鏈數據智能分析平台，為Web3生態建立了一套「智能合約安全-反洗錢合規-虛擬資產犯罪預防和治理」的完整監管技術體系，並與包括中國大陸、香港警務處等在內的全球20多個國家和地區的執法機構緊密合作，同時為200多家虛擬資產服務提供商（VASP）提供KYT反洗錢技術和合規培訓服務，助力Web3生態的安全與合規發展。

While AI and blockchain are accelerating the digital economy, they are also fuelling the internationalisation, automation, scaling, and concealment of cybercrime. Over 80% of emerging cybercrimes now involve virtual assets, with AI enabling hyper-realistic phishing scams, forged KYC documents, and deepfake audio/video scams. These innovations are outpacing traditional security defences.

At Beosin, we pioneer integrated solutions by combining AI and large-language models (LLMs) to build advanced blockchain data intelligence platforms. We have established a comprehensive regulatory technology framework for the Web3 ecosystem covering smart contract security, AML compliance, and virtual asset crime prevention and mitigation. We actively collaborate with law enforcement agencies across 20+ countries and jurisdictions, including the Mainland and HKPF, and provide “Know Your Transaction (KYT)” AML technology and compliance training to 200+ Virtual Asset Service Providers (VASPs) worldwide, supporting the secure and compliant development of the Web3 ecosystem.

朱偉年博士
Dr. Welland CHU
國際信息系統審計協會
（中國香港分會）會長
President,
ISACA China Hong Kong Chapter

隨著數碼創新加速發展——尤其體現在自主系統與人工智能技術的深度融合——社會福祉得以持續提升，但網絡安全風險也同時急劇增長。物聯網的普及應用、企業環境中「人類身份」與「機器身份」數量的急劇增加且氾濫的現象、人工智能的武器化，以及對密碼學構成威脅的量子計算技術的出現，這些因素正急劇地擴大攻擊面，產生日益複雜的網絡威脅。

面對這些挑戰，我們需要建立集體防禦機制。國際信息系統審計協會（中國香港分會）深感榮幸能通過推動資訊科技治理、審計、網絡安全及專業發展等一系列戰略措施貢獻力量。我們與香港警務處、國際刑警組織、監管機構及業界夥伴保持緊密合作，對於有效預防、偵測及應對新興網絡威脅發揮著關鍵作用。

As digital innovation accelerates—through autonomous systems and AI-enhanced collaboration—societal wellbeing will continue to improve. Meanwhile, cybersecurity risks are intensifying. Ubiquitous IoT adoption, proliferation of human and machine identities, weaponisation of AI, and emergence of cryptographically relevant quantum computing are dramatically expanding the attack surface and enabling increasingly sophisticated threats. Confronting these challenges requires collective defence. ISACA China HK Chapter is proud to contribute through strategic initiatives advancing IT governance, audit, cybersecurity, and professional development. Our sustained collaboration with the HKPF, INTERPOL, regulators, and industry partners is pivotal to preventing, detecting, and neutralising these emerging cyber threats.

在商業化成功的背後，AI也正被用於網絡犯罪，例如生成式人工智能被用於製作虛假的多媒體資訊以達到詐騙的目的。我們應該加強引入和研發減少人工智能危害的技術和產品，以降低AI應用在推廣時與社會產生的摩擦。

Beneath the success of its commercialisation, AI is also being exploited for cybercrimes. For instance, generative AI is used to create fake multimedia content for fraudulent purposes. We should strengthen the introduction of technologies and products that mitigate the harms caused by AI, so as to reduce the friction between the promotion of AI applications and society.

蕭子豪先生
Mr. XIAO Zihao
瑞萊智慧科技聯合創辦人及技術總監
Co-founder & CTO, RealAI

# 網絡安全主動措施
# Cybersecurity Initiatives

加強國際合作
**Strengthening International Cooperation**

推進網絡防禦準備工作
**Advancing Cyber Defence Readiness**

推廣網絡安全意識與教育
**Promoting Cybersecurity Awareness and Education**

強化公私營合作
**Enhancing Public and Private Sector Collaboration**

推動情報與數據共享
以加強協作式網絡防禦
**Fostering Intelligence and Data Sharing for Collective Cyber Defence**

# 加強國際合作
# Strengthening International Cooperation

## 國際刑警組織網絡罪案專家組
## INTERPOL's Cybercrime Expert Group (CyberEX)

國際刑警組織網絡罪案專家組（專家組）於2025年重啟，成為國際執法機構、學術機構及業界專家合作打擊網絡犯罪的關鍵平台，匯聚來自73個國家和地區逾170名專家，透過經驗交流協助制定全球網絡犯罪對策。會議期間，各地執法機關及私營機構的專家就新興科技犯罪趨勢進行了深入交流。香港代表團亦與多國專家舉行了多邊會談，進一步深化國際合作。

INTERPOL's Cybercrime Expert Group (CyberEX) was relaunched in 2025 as a key platform for international law enforcement agencies (LEAs), academic institutions, and industry experts to collaborate in combatting cybercrime. Bringing together over 170 experts from 73 countries and regions, the platform facilitates the exchange of experience to support the development of global cybercrime strategies. During the conference, experts from LEAs and the private sector engaged in in-depth discussions on emerging trends in technology crime. The Hong Kong delegation also held multilateral discussions with international counterparts, further strengthening international cooperation.

網罪科總警司林焯豪於2025年6月份出席於法國里昂國際刑警組織總部舉行的國際刑警組織網絡罪案專家組（專家組）年度會議。會議期間，總警司林焯豪獲絕大多數成員支持並獲選為專家組主席，於6月26日獲正式任命。

Chief Superintendent (CSP) LAM Cheuk-ho attended the Annual Conference of INTERPOL's Cybercrime Expert Group (CyberEX) held at the INTERPOL's headquarters in Lyon, France in June 2025. During the conference, CSP LAM received the support of the vast majority of members and was elected as the Chairperson of CyberEX, with his official appointment to the role on June 26.

這項任命乃香港警隊在國際合作方面的重要里程碑。在為期兩年的任期內，總警司林焯豪將與來自摩洛哥、加拿大、瑞士及巴西的四名副主席協作，針對專家組的四大策略支柱：安全策略、罪案調查、預防措施及科技賦能，共同推動全球打擊網絡罪案的策略與行動。當選後，總警司林焯豪闡述了透過新世代網絡警政維護網絡安全的願景，強調各地執法機構須持續推動創新及提升應對能力，並呼籲加強國際合作及公私營夥伴關係，共同應對因先進科技被濫用而產生的挑戰。

This appointment marks a significant milestone for the HKPF in international cooperation. During his two-year term, CSP LAM will collaborate with four Vice-chairpersons from Morocco, Canada, Switzerland and Brazil to advance the global fight against cybercrime, focusing on the Group's four strategic pillars: Strategy, Investigation, Prevention and Empowerment. Following his election, CSP LAM articulated his vision of safeguarding cybersecurity through next-generation cyber policing, emphasising the need for LEAs worldwide to continuously foster innovation and enhance response capabilities. He also called for strengthened international cooperation and public-private partnerships to jointly address the challenges arising from the abuse of advanced technologies.


## 第二屆國際刑警組織亞洲及南太平洋科技罪案聯合行動工作組會議
## The 2nd INTERPOL Asia and South Pacific (ASP) Working Group Meeting on Cybercrime for Heads of Units

網罪科人員於2025年7月8日至11日前往越南河內，出席「第二屆國際刑警組織亞洲及南太平洋科技罪案聯合行動工作組會議」，與來自超過24個亞太地區國家及司法管轄區的網絡執法機構高級官員及網絡安全專家共同深化國際合作及提升應對跨境網絡犯罪的執法能力。會上，總警司林焯豪以工作組副主席身份致開幕辭，全面介紹香港警隊在打擊網絡犯罪方面的國際合作成果並展望未來行動方向；網罪科總督察陳鴻亦匯報了香港警隊參與國際刑警協調的聯合執法行動「Operation SECURE」的具體成果。

「Operation SECURE」於2025年1月至4月期間展開，旨在摧毀與資料盜取相關的網絡犯罪基礎設施。行動中，網罪科分析了逾1 700條情報，並與26個國家的執法部門協作，成功剷除超過兩萬個惡意網絡平台，合共涉及全球超過21.6萬名受害人，並查封41台黑客伺服器，於多個司法管轄區拘捕32名疑犯。



CSTCB participated in the 2nd INTERPOL Asia and South Pacific (ASP) Working Group Meeting on Cybercrime for Heads of Units in Hanoi, Vietnam from 8 to 11 July 2025, joining senior officials from cyber enforcement agencies and cybersecurity experts representing over 24 countries and jurisdictions across the Asia-Pacific region to deepen international cooperation and enhance law enforcement capabilities in combating cross-border cybercrime. At the meeting, CSP LAM Cheuk-ho delivered the opening speech in his capacity as Vice-Chairperson of the Working Group, presenting the HKPF's achievements in international collaboration against cybercrime and outlining future operational directions, while Chief Inspector CHAN Hung reported on the Force's participation and specific results in Operation SECURE, a global joint law enforcement operation coordinated by INTERPOL.

Conducted from January to April 2025, Operation SECURE aimed to dismantle cybercrime infrastructure associated with data theft. CSTCB analysed over 1,700 pieces of intelligence and collaborated with law enforcement agencies from 26 countries, successfully dismantling more than 20,000 malicious online platforms that had affected over 216,000 victims worldwide, seizing 41 hacker servers, and arresting 32 suspects across multiple jurisdictions.

## 第15屆國際刑警組織網絡罪案首長級工作坊及國際網絡罪案應變研討會
## The 15th INTERPOL Cybercrime Directors' Workshop and the International Symposium on Cybercrime Response 2025

於2025年8月份，網罪科人員出席於南韓首爾舉行的「第15屆國際刑警組織網絡罪案首長級工作坊」（工作坊）及「國際網絡罪案應變研討會」（研討會）。是次工作坊以「行動一致：共禦威脅，共塑應變」為主題，匯聚了來自國際刑警組織及亞太區五個司法管轄區的網絡罪案首長級人員，包括南韓、日本、新加坡、香港及以線上參與的中國內地，讓各地區代表積極交流最新的網絡罪案形勢、犯罪手法及應對策略。


會上，總警司林焯豪闡述了網罪科如何應用人工智能技術強化情報處理、網絡威脅分析及針對釣魚詐騙的預警干預；警司張巧儀則與南韓警察廳進行雙邊案件研討，藉國際合作提升調查效能。此外，在主題為「建立網絡信任：共享安全環境」的研討會上，高級督察蘇裕天獲邀分享無人機安全漏洞的數碼法理研究成果，闡述常見漏洞並提供相關事故的調查方案。

In August 2025, CSTCB officers attended the 15th INTERPOL Cybercrime Directors' Workshop (Workshop) and the International Symposium on Cybercrime Response 2025 (Symposium) in Seoul, South Korea. Themed "Working as One: Sharing Threats, Shaping Responses", the Workshop brought together INTERPOL officers and Cybercrime Directors from five jurisdictions in the Asia-Pacific region, namely South Korea, Japan, Singapore, Hong Kong, and Mainland China (participating online), enabling regional representatives to actively exchange insights on the latest cybercrime landscape, criminal methodologies, and response strategies.

During the session, CSP LAM elaborated on CSTCB's application of AI technologies to strengthen intelligence processing, cyber threat analytics, and predictive intervention against phishing scams, while SP CHEUNG held a bilateral case discussion with the Korean National Police Agency to enhance investigation capabilities through international collaboration. At the Symposium, themed "Trust in Cyberspace: Safety for All", SIP SO was invited to share his digital forensics research on drone security vulnerabilities, outlining common system weaknesses and offering investigative approaches to drone-related incidents.

## 網絡指揮官課程
## Cyber Command Course

「網絡指揮官課程」乃專為全球執法機關指揮人員而設的旗艦培訓項目，過往由網罪科與國際刑警組織合辦，旨在於日益互聯的數碼時代中，建立一個跨越國界的網絡防衛能力培訓平台，共同應對由無遠弗屆的網絡罪案所帶來的挑戰。

2026年網絡指揮官課程再次於香港舉辦，本屆課程聚焦於國際網絡黑灰產業鏈，強調國際深度協作和堅實的公私營夥伴合作互通的重要性，並探討由新興技術如人工智能及加密貨幣所帶來的挑戰。課程旨在提升指揮人員在處理複雜跨國網絡罪案時的戰略領導能力與宏觀視野，同時探討如何將新科技融入日常警務行動及資源管理之中。

此外，課程亦展示了香港警務處正轉型為一支具備創新思維、重視人才培訓與變革管理、並擁有持續學習文化的現代化警隊。


The Cyber Command Course is a flagship training programme designed specifically for commanders from LEAs around the world. Previously co-organised by CSTCB and INTERPOL, the course aims to build cross-border cyber defence capabilities in an increasingly interconnected digital era, and to jointly tackle the growing challenges posed by borderless cybercrimes.

The Cyber Command Course 2026 was held once again in Hong Kong. This year's programme focused on the international cybercrime ecosystem, emphasising the importance of deeper international cooperation and robust public-private partnerships. It also examined the challenges posed by emerging technologies such as artificial intelligence and cryptocurrencies. Designed to enhance participants' strategic leadership and broader perspective in handling complex transnational cybercrimes, the course also explored how new technologies could be integrated into day-to-day policing operations and resource management.

Furthermore, the programme also showcased how the HKPF is transforming into a modern, innovation-driven police service that places strong emphasis on talent development and change management, and fosters a culture of continuous learning.

## 第十屆數碼法理鑑證專家小組會議
## The 10th Digital Forensics Expert Group Meeting (DFEG 2025)

由國際刑警組織主辦，網罪科與香港大學協辦的「第十屆數碼法理鑑證專家小組會議」，於2025年7月14日至16日在香港大學舉行。該活動為首次在香港舉行，吸引超過40個國家及地區、共100多名相關學術及執法機構的專家參與。會議共邀請了27名專家，圍繞最新科技發展、取證技術及人工智能應用等議題進行了深入探討，共同推動全球數碼法證專業發展。此次活動同時彰顯香港在推動國際數碼法證專業交流方面的積極角色。



The 10th Digital Forensics Expert Group Meeting (DFEG 2025), hosted by INTERPOL and co-organised by CSTCB and the University of Hong Kong (HKU), was held at HKU from 14 to 16 July 2025. Marking its inaugural hosting in Hong Kong, the event attracted over 100 experts from more than 40 countries and regions, representing relevant academic and law enforcement institutions. DFEG 2025 featured presentations and in-depth discussions by 27 experts on topics such as the latest technological developments, forensic techniques, and applications of artificial intelligence (AI), collectively advancing the global digital forensics profession. The event also highlighted Hong Kong's active role in promoting international exchange within the field of digital forensics.



## 第二屆「國際數碼鑑證挑戰賽」
## The 2nd International Digital Forensics Challenge (IDFC 2025)

網罪科聯同香港大學及Dataport Technology Limited 協辦的第二屆「國際數碼鑑證挑戰賽」(IDFC 2025)於2025年7月16日至17日圓滿舉行。本年度賽事匯聚了來自15個地區的22支隊伍，參賽者背景多元，涵蓋執法機構、學術界及數碼鑑證專業人士，充分展示各地在科技罪案調查領域的專業實力。

比賽以一宗模擬個案為主題，其情節設定為某投資公司的人工智能模型遭黑客入侵，並被利用來設計虛假的投資計劃，以誘使投資者購買不存在的加密貨幣。參賽隊伍需在限時內分析電子證據、追蹤虛擬資產流向及重構案件過程，全面考驗參加者在數碼鑑證及網絡安全領域的專業知識與應變能力。

此次挑戰賽除提升參賽者的實戰經驗外，亦有效促進了國際間在打擊網絡及金融科技罪行方面的交流與合作。經過激烈角逐，香港海關隊伍憑藉出色的技術水平及協作精神，成功奪得總冠軍。

CSTCB, in collaboration with HKU and Dataport Technology Limited, successfully co-hosted the 2nd International Digital Forensics Challenge (IDFC 2025) from 16 to 17 July 2025. The event brought together 22 teams from 15 regions, comprising a diverse range of participants from law enforcement agencies, academic institutions, and digital forensics professionals worldwide, effectively showcasing their expertise in technology crime investigation.

The competition centred on a simulated cybercrime scenario in which an investment company's AI model was compromised and exploited to create a fictitious cryptocurrency investment scheme, luring investors into purchasing non-existent digital assets. Participants were tasked with analysing digital evidence, tracing virtual asset flows, and reconstructing the incident within a strict timeframe, thereby comprehensively testing their professional knowledge and response capabilities in the fields of digital forensics and cybersecurity.

Beyond enhancing the participants' practical experience, the challenge also effectively fostered international exchange and cooperation in combating cyber-enabled financial crimes. After intense competition, the team from the Hong Kong Customs and Excise Department emerged as the overall champion, demonstrating exceptional technical proficiency and teamwork.


## 與國際刑警組織合作打擊網絡釣魚
## Collaboration with INTERPOL to Combat Phishing

網罪科持續積極參與由國際刑警組織主導、旨在打擊跨國網絡釣魚的行動。透過既有的情報共享渠道及積極參與案件協調會議，我們為全球合力打擊釣魚網絡、提升集體網絡安全防護能力的聯合行動作出實質貢獻。網罪科更擔任國際刑警組織亞洲及南太平洋科技罪案聯合行動工作組轄下打擊網絡釣魚行動組組長，專門負責統籌及協調區內應對相關威脅的行動。

CSTCB continues to actively participate in INTERPOL-led operations aimed at combating transnational phishing. By leveraging established intelligence-sharing channels and actively engaging in case coordination meetings, we contribute substantively to global joint efforts to disrupt phishing networks and enhance collective cybersecurity resilience. CSTCB has also taken the lead of the operation sub-group on phishing under the INTERPOL Asia and South Pacific Joint Operations on Cybercrime Working Group to coordinate regional actions against threats relating to phishing.

## 第五十屆日內瓦國際發明展
## The 50th International Exhibition of Inventions of Geneva


網罪科人員2025年4月份在瑞士日內瓦參與第五十屆日內瓦國際發明展，奪得佳績，首次勇奪由現場國際媒體代表投票評選的「國際傳媒大獎」、另外獲得一項「評審團嘉許金獎」，以及一金、一銀的國際獎項，包括:

(一)「防騙視伏器系列」– 集手機應用程式、防騙資料搜索引擎及銀行可疑交易高危警示於一體，實時偵測詐騙行為，讓市民在點擊轉賬前已能洞察風險，防患於未然(國際傳媒大獎及金獎)

(二) CryptoTrace – 與香港大學攜手研發，運用先進的區塊鏈分析技術，有效追蹤涉及案件的虛擬貨幣交易，準確提取關鍵調查線索，為前線人員調查科技罪案提供支援，簡化虛擬貨幣相關騙案的調查流程(評審團嘉許金獎)

(三) RAPID引擎 – 透過多機構合作及多來源的主動偵測，對新註冊的可疑網站進行檢測，運用人工智能演算法從域名特徵及可疑代碼等多維規則進行即時分析，同步將威脅情報更新至「防騙視伏器」，並傳送至多家網絡服務供應商以進行封鎖，有效強化大眾抵禦釣魚網站的能力(銀獎)。

這些獎項充分展現了香港警隊致力利用創新科技推動智慧警政和提升警務效率的堅定承諾。警隊有效運用人工智能技術，幫助市民預防詐騙，並在加強執法能力方面取得顯著成效，特別是在打擊虛擬資產等新型犯罪領域，積極應對不斷變化的犯罪模式。

Officers of CSTCB reached new heights at the 50th International Exhibition of Inventions of Geneva, which was held in April 2025 in Geneva, Switzerland, and garnered the "International Press Prize" for the first time, the "Gold Medal with the Congratulations of Jury", along with one Gold, and one Silver international award, including:

(1) Scameter Series – A multi-layered public anti-scam initiative comprising a public-facing mobile app with real-time scam detection, open-data policies sharing threat intelligence with strategic stakeholders, and partnerships with banks to send public alerts on high-risk transactions (International Press Prize & Gold Medal)

(2) CryptoTrace – Jointly developed with the University of Hong Kong, this cutting-edge virtual asset analytics platform facilitates cryptocurrency tracing, fund flow analysis, and wallet correlation, accelerating fraud detection for frontline investigators (Gold Medal with the Congratulations of Jury)

(3) RAPID Engine – Through multilateral collaboration and proactive detection from various sources, RAPID Engine inspects on newly registered suspicious websites. Utilising AI algorithms, RAPID Engine performs real-time analysis based on multidimensional rules such as domain characteristics and suspicious codes. Threat intelligence is simultaneously updated to the "Scameter Series" and sent to multiple internet service providers for blocking, effectively enhancing the public's ability to resist phishing threats (Silver Medal)

The awards demonstrate the Force's commitment to leveraging innovative technology to promote smart policing and improve operational efficiency. Additionally, the Force effectively employs AI to assist the public in combating fraud and enhancing law enforcement capabilities, particularly in tackling emerging types of crimes, including those related to virtual assets.



# 推進網絡防禦準備工作
# Advancing Cyber Defence Readiness

## 網絡安全研討會
## Cyber Security Seminars

為加強公私營機構對新興網絡威脅的認知及應對能力，網罪科於 2025 年 3 月及 10 月舉辦了兩場網絡安全研討會，合共吸引超過 100 間公私營機構的代表參與。研討會透過分享網絡威脅情報、實務經驗及防禦策略，有效加強跨界別交流與協作，並促進威脅情報的實務應用，從而提升整體網絡安全防禦能力，為維護香港網絡空間的安全與穩定作出貢獻。


To enhance awareness of and response capabilities against emerging cyber threats among public and private sector organisations, CSTCB organised two cybersecurity seminars in March and October 2025, attracting participation from representatives of over 100 public and private organisations. Through the sharing of cyber threat intelligence, practical experience and defensive strategies, these seminars strengthened cross-sector communication and collaboration, facilitated the practical application of threat intelligence, and thereby enhanced overall cybersecurity defence capabilities, contributing to the safety and stability of Hong Kong's cyberspace.

## 網絡攻防精英培訓暨攻防大賽 2025
## Cyber Attack and Defence Elite Training cum Tournament (CADET) 2025

為提升網絡安全人員的攻防能力，網罪科於2025年7月舉辦了為期三日的「網絡攻防精英培訓暨攻防大賽 2025」。該活動不僅提供培訓，更透過模擬網絡攻擊的比賽，提升從業人員的專業技能及網絡事故應變能力，以全面加強香港的網絡安全。活動期間，共有超過50間機構、合共130名從業員接受攻防培訓；同時，攻防比賽更吸引超過400支隊伍、合共1 400名業界與學界精英踴躍參與。



To enhance offensive and defensive capabilities of cybersecurity personnel, CSTCB organised the three-day "Cyber Attack and Defence Elite Training cum Tournament 2025" (CADET 2025) in July 2025. The programme not only provided training, but also enhanced practitioners' professional skills and cyber incident response capabilities through simulated cyberattack competitions, thereby comprehensively strengthening cybersecurity in Hong Kong. During the event, attack and defence training was provided to 130 personnel from more than 50 organisations. Concurrently, the tournament attracted over 400 teams, comprising 1,400 industry and academic elites, who actively participated in the competition.

## 網絡安全多元創新論壇2025
## Cybersecurity & Diverse Innovation Symposium 2025

由網罪科與數字政策辦公室合辦的「網絡安全多元創新論壇2025」於5月16日假香港會議展覽中心舉行，匯聚逾600名來自政府、業界及學界的代表。警務處處長周一鳴在開幕致辭中指出，當前問題已不是攻擊會否發生，而是何時發生及我們的準備程度。論壇邀請逾30位講者，設有主題演講及六場專題討論，議題涵蓋人工智能治理、供應鏈安全、可信平台部署、跨界協作及新興攻擊趨勢等，為與會者提供了交流實務經驗、強化合作關係及協調跨領域策略的平台，從而提升香港在預防、偵測及應對網絡威脅方面的能力。網罪科與數字政策辦公室重申將持續投入，致力構建一個安全、創新且具韌性的數碼生態系統。

Co-organised by CSTCB and the Digital Policy Office, the Cybersecurity & Diverse Innovation Symposium 2025 was held on 16 May at the Hong Kong Convention and Exhibition Centre, bringing together over 600 participants from government, industry and academia. In his opening remarks, Commissioner of Police Mr CHOW Yat-ming, Joe, highlighted that the critical question is no longer whether cyberattacks will occur, but when—and how prepared we are. Featuring over 30 speakers, the Symposium included keynote sessions and six panel discussions on topics such as AI governance, supply-chain security, trusted platform deployment, cross-sector collaboration, and emerging attack trends. The event served as a platform for exchanging practical experience, strengthening partnerships, and aligning strategies across sectors, thereby enhancing Hong Kong's capability to prevent, detect, and respond to cyber threats. CSTCB and the Digital Policy Office reaffirmed their commitment to sustained engagement to build a secure, innovative and resilient digital ecosystem.


## 第九屆跨部門網絡安全演習
## The 9th Inter-departmental Cyber Security Drill

為提升政府部門應對網絡威脅的整體能力，網罪科與數字政策辦公室於2025年5月合辦了第九屆「跨部門網絡安全演習」，吸引超過280名來自71個政府部門及六個專業及學術機構的資訊科技專業人員及業界專家參與。《行政長官2024年施政報告》宣布引入「三層防範機制」以加強反恐工作。據此，今屆演習首次增設反恐專題環節「跨部門反恐暨資訊科技安全挑戰賽」及「網絡防禦挑戰賽」，以強化政府應對網絡恐怖主義威脅的整體防禦實力，以及提升人員處理網絡安全事件的能力。


To strengthen the government's overall capability to counter cyber threats, CSTCB and the Digital Policy Office co-organised the 9th Inter-Departmental Cyber Security Drill in May 2025. The exercise attracted over 280 IT professionals and industry experts from 71 government departments and six professional and academic institutions. "The Chief Executive's 2024 Policy Address" announced the introduction of the "Three-tier Prevention Framework" to enhance counter-terrorism efforts. In line with this, this year's drill, for the first time, incorporated a counter-terrorism segment comprising the "Counter-Terrorism Information Security Awareness Challenge" and the "Cyber Defence Tournament", aiming to bolster the government's overall defence capabilities against cyber terrorism threats and enhance personnel's ability to handle cybersecurity incidents.



## 「狩網運動2025」
## BugHunting Campaign 2025

網罪科自2023年起與一家本地眾包網絡安全漏洞檢測平台Cyberbay合辦「狩網運動」，並自2024年起與個人資料私隱專員公署建立戰略夥伴關係。該活動已連續三年透過網絡漏洞檢測，為本地機構及企業提升網絡安全防護能力。

「狩網運動2025」於2025年7至8月舉行，吸引185間機構參與，涵蓋銀行與金融服務、醫療保健服務、教育、科技、中小企等多個行業。活動利用人工智能技術及匯聚網絡安全專才，為參與機構提供更全面的網絡安全漏洞測試、安全報告及一對一的專業諮詢服務。網罪科期望未來能擴大活動的覆蓋面，讓更多不同機構參與，從而推動企業系統漏洞檢測的普及化，攜手共建更安全的數碼網絡環境。



CSTCB has organised the BugHunting Campaign in collaboration with the local crowdsourced cybersecurity company Cyberbay since 2023 and has entered into a strategic partnership with PCPD since 2024. For three consecutive years, the campaign has helped local organisations and enterprises enhance their cybersecurity defences through vulnerability testing.

The BugHunting Campaign 2025 was conducted from July to August 2025, with participation from 185 organisations across sectors such as banking and financial services, healthcare services, education, technology, and SMEs. Leveraging artificial intelligence technology and the expertise of cybersecurity professionals, the campaign provided participants with comprehensive vulnerability testing, security reports, and one-on-one professional consultation services. CSTCB aims to expand the campaign's reach to involve a wider range of organisations in the future, thereby promoting the widespread adoption of system vulnerability testing for enterprises and jointly building a more secure digital network environment.

## 「釣魚電郵演習2025」
## Ethical Phishing Email Campaign 2025

為提升員工識別可疑電郵的意識，並降低參與機構的網絡安全風險，網罪科自2021年起舉辦「釣魚電郵演習」，並於2023年開始與香港互聯網註冊管理有限公司合辦該活動，及至2025年更與個人資料私隱專員公署結為策略夥伴。

第五屆「釣魚電郵演習」於2025年10月至2026年1月期間舉行，共吸引了來自301間機構的53 285名參與者。演習期間，參與機構的員工收到四封模擬釣魚電郵，旨在測試其網絡安全意識。本屆新增釣魚短訊演習，共吸引30間機構的3 620名參與者。活動結束後，每間參與機構均收到一份詳細報告，當中列明其員工在處理可疑電郵及短訊方面的整體表現。此項演習旨在提高企業員工對釣魚攻擊的防範意識，為共同構建一個更安全、更具韌性的香港網絡安全環境作出貢獻。


To raise staff awareness in identifying suspicious emails and reduce cybersecurity risks for participating organisations, CSTCB has organised the Ethical Phishing Email Campaign since 2021, collaborated with the HKIRC since 2023, and welcomed PCPD as a strategic partner in 2025.

The 5th Ethical Phishing Email Campaign was held from October 2025 to January 2026, which attracted 53,285 participants from 301 organisations. During the campaign, employees from participating organisations received four pseudo-phishing emails designed to assess their cybersecurity awareness. Additionally, a phishing SMS campaign was newly introduced this year which attracted 30 organisations with 3,620 participants. Upon conclusion of the campaign, each participating organisation received a comprehensive report that detailed the overall performance of its employees in handling suspicious emails and SMS. The campaign seeks to raise awareness among corporate employees against phishing attacks and contributes to building a safer and more resilient cybersecurity environment in Hong Kong.

## 網絡安全研討會暨「舉劍者」桌上演練
## Cyber Security Seminar cum Tabletop Exercise "SWORDLIFTER"

網罪科於2025年9月9日舉辦代號為「舉劍者」的網絡安全研討會暨桌上演練。活動旨在提升相關持份者在籌備第十五屆全國運動會(十五運會)及全國第十二屆殘疾人運動會暨第九屆特殊奧林匹克運動會(殘特奧會)期間的網絡韌性、事故通報協調及即時應對能力。

CSTCB organised the Cyber Security Seminar cum Tabletop Exercise, codenamed SWORDLIFTER, on 9 September 2025, aiming to strengthen the cyber resilience, incident-reporting coordination, and immediate response capabilities of key stakeholders in preparation for the 15th National Games, the 12th National Games for Persons with Disabilities and the 9th National Special Olympic Games.

是次研討會內容涵蓋大型體育賽事相關的網絡威脅態勢及防禦策略，討論議題廣泛，包括防範網絡釣魚、系統入侵防護，以及網站、應用系統和社交媒體帳戶的安全管理。來自業界的專家分享了本地與海外的實戰經驗，提供實用的見解與最佳實踐，從而有助提升所有持份者的網絡安全意識並強化預防措施。

The seminar covered cyber-threat landscape and defence strategies associated with major sporting events, addressing a wide range of topics including phishing prevention, system intrusion protection, and the security of websites, applications, and social media accounts. Industry experts shared practical experience from both local and overseas contexts, offering valuable insights and best practices, thereby helping to raise awareness and reinforce preventive measures across all stakeholder groups.

隨後進行的桌上演練以綜合情境模擬賽前可能發生的網絡事故，並根據各參與機構的業務環境量身訂製獨特的情境，要求他們進行事故分析、執行跨機構協調通報，以及開展復原與系統恢復工作。透過這次實戰模擬，持份者能夠更清晰地理解各類網絡攻擊的潛在影響及相應的應對流程。

The accompanying tabletop exercise featured an integrated scenario simulating potential pre-event cyber incidents. Tailored to the unique operational contexts of each participating organisation, the scenarios required participants to perform incident analysis, execute coordinated multi-agency reporting procedures, and undertake recovery and service-restoration operations. Through this hands-on simulation, stakeholders gained a clearer understanding of the potential impacts of various cyberattacks and the corresponding response workflows.

是次活動吸引了逾 30 個部門和機構、超過 100 名代表參與，包括全國運動會香港賽區統籌辦公室、場館營運者、政府部門、運輸及公共事業機構，以及相關體育總會等。活動不僅有效提升了相關組織的網絡安全標準，也促進了更強的跨界別溝通與協作，確保所有相關方為保障十五運會及殘特奧會的網絡安全完整性做好更充分的準備。

The event attracted over 100 representatives from more than 30 departments and organisations, including the National Games Coordination Office (Hong Kong), venue operators, government departments, transportation and public bodies, as well as relevant sports associations. It not only enhanced the cybersecurity standards of the organisations involved, but also fostered stronger cross-sector communication and collaboration, ensuring that all parties are better prepared to safeguard the integrity of the upcoming Games.

# 推廣網絡安全意識與教育
# Promoting Cybersecurity Awareness and Education

## 守網聯盟2025
## CyberDefence Campaign 2025

「守網聯盟」是網罪科其中一個重點協作項目，匯聚超過130個政府部門、公營機構及私人企業，各夥伴在其所屬領域貢獻力量，共同提升本港網絡安全及防騙能力。

The "CyberDefenders' Alliance" is one of the key collaborative initiatives led by CSTCB, bringing together more than 130 government departments, public bodies, and private corporations. Each partner contributes within its respective sector to collectively strengthen Hong Kong's cybersecurity and anti-deception capabilities.

2025年10月，網罪科透過「守網聯盟」平台推出「守網聯盟遊戲卡」。此計劃由網罪科聯同教育局及數字政策辦公室共同籌辦，並在全港中小學進行積極推廣，旨在系統性地培養青少年的網絡安全意識，為社區數碼素養的長遠提升作出貢獻。

In October 2025, CSTCB launched the "CyberDefenders' Alliance Card Game" through the Alliance's platform. This program is jointly organised by CSTCB, the Education Bureau, and the Digital Policy Office, and is being promoted actively across all primary and secondary schools in Hong Kong. It aims to systematically cultivate cybersecurity awareness among young people and contribute to the long-term advancement of digital literacy in the community.


每一張遊戲卡均精心設計，內容包含基於真實案件的網絡安全資訊，並對應已知的犯案手法。玩家透過策略性地組合不同的遊戲卡，進行戰術部署及結構化的攻防戰，並在沉浸式的互動學習體驗中深刻理解網絡威脅並掌握相應的防禦技能，從而實現教育與實踐體驗的深度融合。

Each game card is thoughtfully designed, containing cybersecurity content based on authentic real-world cases and recognised criminal tactics. By strategically combining different cards to simulate tactical deployments and conduct structured attack-defence exercises, participants engage in an interactive and immersive learning experience. This approach not only deepens their practical understanding of cyber threats, but also builds applicable defensive skills, achieving a deliberate fusion of education and experiential engagement.

其中，「特別超級稀有」及「極稀有」遊戲卡更印有參與部門及機構的吉祥物，極具吸引力與收藏價值。我們希望市民在參與遊戲的同時，將這些卡牌作為實用且令人印象深刻的教育工具予以珍藏，從而逐步建立社區必要的數碼素養，並培養對網絡威脅的持久警惕性。

The "Super Special Rare" and "Ultra Rare" card sets are printed with mascots from participating departments and organisations, significantly enhancing their appeal and collectability. This design is intended not only to engage the public through gameplay, but also to encourage them to retain these cards as practical and memorable educational tools. Thereby, it seeks to steadily build essential digital literacy across the community and cultivate sustained alertness to cyber threats.

## 大灣區青少年人工智能及網絡安全挑戰賽2025
## Greater Bay Area Youth AI and CyberSec Challenge 2025

由網罪科聯同澳門司法警察局（司警局）及教育及青年發展局聯合主辦的「大灣區青少年人工智能及網絡安全挑戰賽2025」決賽暨頒獎禮，於2026年3月9日在香港圓滿舉行。比賽旨在鼓勵大灣區青年緊貼科技步伐，提升網絡安全防範意識，並透過交流為未來構建安全穩健的數碼環境培育人才。

The Final and Awards Ceremony of the "Greater Bay Area Youth AI and Cybersecurity Challenge 2025" concluded successfully in Hong Kong on March 9, 2026. The event was jointly organised by CSTCB, the Judiciary Police of Macao, and the Education and Youth Development Bureau of Macao. The competition aimed to encourage youth in the Greater Bay Area (GBA) to keep pace with technological advancements, enhance cybersecurity awareness, and cultivate talent for a secure digital future through cross-border exchange.


是次挑戰賽由香港教育局、資訊科技教育領袖協會、廣州市人工智能產業發展促進會、香港資訊科技學院、澳門科學館及中國移動（國際）有限公司協辦，吸引粵港澳三地共1 100名學生報名。經初賽甄選後，52名香港、46名澳門及22名內地學生脫穎而出，齊集香港參與三日兩夜的「人工智能訓練營」及決賽。120名精英學生經隨機抽籤組成跨地區隊伍，接受人工智能、網絡安全及團隊溝通等全方位培訓。今年賽事特別著重創新與實踐結合，題目加入豐富商業元素，鼓勵學生跳出框架，從實際應用和商業價值角度構思並製作實用的參賽模型。

The challenge was co-organised by the Education Bureau of Hong Kong, the Association of IT Leaders in Education, the Guangzhou AI Industry Development Promotion Association, the Hong Kong Institute of Information Technology, the Macao Science Center, and China Mobile International Limited. It attracted 1,100 student applicants from Guangdong, Hong Kong, and Macao. Following the preliminary rounds, 120 elite students—comprising 52 from Hong Kong, 46 from Macao, and 22 from the Mainland—were selected to attend a three-day, two-night "AI Training Camp" and the final competition in Hong Kong. These students were randomly assigned to inter-regional teams to receive comprehensive training in AI, cybersecurity, and team communication. This year's competition emphasised the integration of innovation and practice, incorporating commercial elements to encourage students to think beyond conventional boundaries and develop practical models with real-world application and business value.

是次比賽為大灣區青少年提供優質交流平台，不僅提升新一代網絡素養，更為他們應對未來數碼挑戰及投身科研發展奠定堅實基礎。

This competition provided a high-quality exchange platform for GBA youth, enhancing the digital literacy of the next generation and building a solid foundation for their future in scientific research and digital challenges.

## 滅罪精英運動會
## Anti-Crime Elite Games Carnival

網罪科聯同刑事部轄下的商業罪案調查科、家庭衝突及性暴力政策組、財富情報及調查科及毒品調查科，於2025年10月18日及19日在西九文化區舉辦「滅罪精英運動會」，吸引逾二萬名市民入場。現場氣氛熱烈，節目豐富，包括警察樂隊演奏、警犬隊示範，以及多項音樂、舞蹈和魔術表演。在網罪科展區，我們邀請了包括澳門科學館在內的11個策略夥伴及科技機構設立攤位遊戲，並特設「守網聯盟遊戲卡」攤位，讓市民現場收集卡牌及對戰，以生動互動的形式傳遞反詐騙及網絡安全信息，提升大眾對網絡陷阱的警覺性。

CSTCB, together with the Commercial Crime Bureau (CCB), Family Conflict and Sexual Violence Policy Unit (FCSV), Financial Intelligence and Investigation Bureau (FIIB), and Narcotics Bureau (NB) under Crime Wing, organised the "Anti-Crime Elite Games" on 18 and 19 October 2025 at the West Kowloon Cultural District, attracting over 20,000 visitors. The vibrant event featured performances by the Police Band and Police Dog Unit, alongside music, dance, and magic shows. In the CSTCB zone, 11 strategic partners and technology organisations — including the Macao Science Center — hosted game booths, with a dedicated "CyberDefenders' Alliance Card Game" booth where visitors could collect cards and engage in on-site battles, disseminating anti-scam and cybersecurity messages through interactive gameplay to raise public awareness of online threats.

## 香港學校網絡安全指南
## Cybersecurity Guidebook for Schools in Hong Kong

網罪科一直重視校園網絡安全建設，並積極透過跨界別協作提升學界的網絡安全韌性。為此，我們聯同香港互聯網註冊管理有限公司、資訊科技教育領袖協會（AiTLE）及羅兵咸永道香港 DarkLab 合作編製《香港學校網絡安全指南》（下稱《指南》），為本地學校提供實用且系統化的參考框架。《指南》聚焦四大範疇，包括政策與制度範本、真實案例分析、事故應變流程，以及系統與網絡配置建議清單，協助資源及技術能力各異的學校，將網絡安全要求融入日常管理與教學運作，逐步建立有效的防護能力。


為配合《指南》發布，網罪科亦舉辦「校園網安講座」，與合作機構專家共同分享最新威脅趨勢、常見攻擊手法及校園防護建議，並與逾50間本地學校的教師交流，提升學界對網安風險的認知，加強新學年前的防護準備。展望未來，網罪科將繼續與業界、學界及專業機構緊密合作，推動校園網絡安全能力建設，助力學校在安全可靠的數碼環境中推動創新教學，為香港整體的數碼素養與網絡韌性奠定更穩固基礎。

CSTCB places strong emphasis on strengthening cybersecurity within the school sector and actively enhances cyber resilience in education through cross-sector collaboration. To this end, we collaborated with the HKIRC, the Association of I.T. Leaders in Education (AiTLE), and PwC Hong Kong DarkLab to publish the Cybersecurity Guidebook for Schools in Hong Kong ("the Guidebook"), providing local schools with a practical and systematic reference framework. The Guidebook focuses on four key areas — policy and governance templates, real-world case studies, incident response workflows, and system/network configuration checklists — helping schools of varying resources and technical capability embed cybersecurity into daily management and teaching operations, and progressively build effective defences.

To complement the release, CSTCB also organised a School Cybersecurity Seminar, where partner experts shared the latest threat trends, common attack patterns, and practical security recommendations, engaging teachers from over 50 local schools to raise awareness of cyber risks and strengthen preparedness ahead of the new academic year. Looking ahead, CSTCB will continue to work closely with industry, the education sector, and professional organisations to advance cybersecurity capacity-building in schools, supporting innovative teaching in a secure digital environment and laying a stronger foundation for digital literacy and cyber resilience across Hong Kong.

# 強化公私營合作
# Enhancing Public and Private Sector Collaboration

## 網絡安全精英嘉許計劃2025
## Cyber Security Professional Awards 2025

《網絡安全精英嘉許計劃2025》是由香港警務處網罪科主辦，與數字政策辦公室（政府電腦保安事故協調中心）和香港生產力促進局（香港網絡安全事故協調中心）協辦的一項備受推崇的獎項計劃。該獎項旨在表彰在政策實施、風險管理、事故應對、網絡防禦創新以及推廣強大的網絡安全文化等領域表現卓越的個人和機構。本次評選共收到來自140個機構的219份提名，充分展示了業界對此盛事的廣泛參與。

The Cyber Security Professional Awards 2025 (CSPA 2025) is a prestigious award programme organised by CSTCB, and co-organised by the Digital Policy Office (Government Computer Emergency Response Team Hong Kong) and Hong Kong Productivity Council (Hong Kong Computer Emergency Response Team Coordination Centre). The Awards recognise individuals and organisations that have demonstrated excellence in areas such as policy implementation, risk management, incident response, cyber defence innovation, and the promotion of a strong cybersecurity culture. A total of 219 nominations were received from 140 organisations, underscoring broad industry participation in this distinguished event.



## 網絡安全特別行動小組
## Cyber Security Action Task Force (CSATF)

香港警務處於2024年成立網絡安全特別行動小組，集合全球資深網絡安全專家及企業，與執法機構緊密合作，共同打擊網絡犯罪。該小組旨在加強網絡威脅情報共享、提升行動支援，並推動專業知識共享，從而有效提升未來應對不斷演變的網絡威脅的整體能力。

In 2024, the HKPF established the Cyber Security Action Task Force (CSATF), bringing together leading global cybersecurity experts and firms to work closely with law enforcement agencies in combating cybercrime. The Task Force aims to strengthen cyber threat intelligence sharing, enhance operational support, and promote professional knowledge exchange, ultimately boosting the collective capability to effectively respond to evolving cyber threats in the future.


「網絡安全精英嘉許計劃2025」頒獎典禮於2026年1月舉行，典禮期間同時舉行了「網絡安全特別行動小組」第二屆成員的就職儀式。來自海內外的 12家網絡安全行業的資深機構獲委任加入該小組，任期為兩年。第二屆行動小組的成立，標誌著公私營機構為共同維護香港網絡安全環境而持續協作。

The Cyber Security Professional Awards 2025 presentation ceremony was held in January 2026, during which the inauguration ceremony for the second term of the CSATF took place. 12 leading cybersecurity firms from around the world were appointed to the CSATF for a two-year term. The establishment of the second term signifies the ongoing collaboration between public and private institutions in their shared commitment to safeguarding Hong Kong's cybersecurity landscape.



## 虛擬資產情報工作組
## Virtual Asset Intelligence Taskforce (VAIT)

為應對虛擬資產相關罪案所帶來的挑戰，網罪科成立「虛擬資產情報工作組」，積極促進執法機構（香港警務處及香港海關）、監管機構（香港金融管理局(金管局）及證券及期貨事務監察委員會（證監會））、持牌虛擬資產服務提供者及持牌穩定幣發行人之間的情報交流與知識共享。工作組透過完善執法協作機制、優化虛擬資產止付流程及加強反洗黑錢工作，致力與各界持份者攜手合作，共同構建一個安全及合規的數字資產行業生態，保障市民免受虛擬資產相關罪案的威脅。



To address the challenges posed by virtual asset-related crimes, CSTCB established the "Virtual Asset Intelligence Taskforce (VAIT)" to promote intelligence exchange and knowledge sharing among law enforcement agencies (HKPF and Hong Kong Customs and Excise Department), regulatory agencies (the Hong Kong Monetary Authority (HKMA) and Securities and Futures Commission (SFC)), licensed Virtual Asset Service Providers, and licensed stablecoin issuers. By enhancing enforcement collaboration mechanisms, optimising virtual asset stop payment procedures and strengthening anti-money laundering efforts, the VAIT is dedicated to collaborating with all stakeholders to build a safe and compliant digital asset industry ecosystem, thereby protecting the public from virtual asset-related crimes.

## 智慧警政顧問小組
## Smart Policing Advisory Panel (SPAP)

於2025年3月成立的第二屆「智慧警政顧問小組」（前稱「科技罪案警政顧問小組」），由警務處刑事及保安處處長擔任主席。該小組由原「科技罪案警政顧問小組」正名，旨在反映其職能與範疇的拓展，工作重點已由科技罪案延伸至更全面的警政議題及新興科技的應用與治理。

「智慧警政顧問小組」成員涵蓋網絡安全、人工智能、區塊鏈、金融科技及低空經濟等多個專業領域。第二屆小組已於2025年舉行四次會議，深入探討了「低空經濟與警政創新」、「低軌衛星與5G/6G的未來發展」，以及「通用人工智能（AGI）與超級人工智能（ASI）的發展」等新興科技議題。

The second-term "Smart Policing Advisory Panel" (formerly known as the "Cybercrime Policing Advisory Panel") was established in March 2025 and is chaired by Director of Crime and Security (D C&S). The panel was renamed from its previous title to reflect the expansion of its functions and scope, with its focus extending beyond technology-related crimes to encompass broader policing issues as well as the application and governance of emerging technologies.

Members of the Smart Policing Advisory Panel come from diverse professional backgrounds, including cybersecurity, artificial intelligence, blockchain, financial technology, and the low-altitude economy. In 2025, the second-term panel convened four meetings, engaging in in-depth discussions on emerging technological topics such as "Low-Altitude Economy and Policing Innovation," "The Future Development of Low-Earth Orbit Satellites and 5G/6G," and "The Development of Artificial General Intelligence (AGI) and Artificial Superintelligence (ASI)."

# 推動情報與數據共享以加強協作式網絡防禦
# Fostering Intelligence and Data Sharing for Collective Cyber Defence

## 「防騙視伏器」升級
## Scameter Enhancement

2025年，警隊為「防騙視伏器」及「防騙視伏App (Scameter+)」進行重大升級，引入 AI+ 分析框架，令詐騙情報的處理、比對和入庫更為自動化及高效。系統能對市民舉報的可疑電話及網址進行快速評估，將多項風險因素整合為統一分析結果，大幅縮短核實時間，令預警更快、更準、更全面。

In 2025, the Police introduced a major upgrade to the "Scameter+" platform, deploying an AI+ analysis framework that significantly enhances the automation and efficiency of scam intelligence processing, matching, and data ingestion. The enhanced system can autonomously assess public reports of suspicious URLs and phone numbers by integrating multiple risk indicators into a unified analysis result. This greatly shortens verification time and enables even faster, more accurate, and more comprehensive scam protection.

升級後的「防騙視伏App」手機應用程式支援自動更新資料庫，並擴展至多個主要社交媒體平台的舉報渠道，讓市民能輕鬆提交各類可疑訊息。由人工智能驅動的提前警示機制亦已投入運作，經核實的高風險項目會即時納入資料庫並標示為「高危」。此外，系統每日整理最新詐騙趨勢，推出「熱門騙局排行榜」，從而加強公眾對新興詐騙手法的認識。

The upgraded Scameter+ mobile app now supports automatic database updates and has expanded its reporting channels to include major social media platforms, allowing the public to easily submit various types of suspicious information. An AI-driven early-warning mechanism is also now operational, with verified high-risk items immediately indexed into the Scameter database and flagged as "high-risk". Furthermore, the system compiles daily updates on the latest scam trends and publishes a prevalent scam ranking, thereby strengthening public awareness of emerging fraudulent tactics.




2025年的另一項重要進展，是「防騙視伏器」數據在金融業務中的深化應用。銀行及金融機構已將高風險電話、電郵、IP及收款帳戶等「防騙視伏器」識別的指標，融入開戶程序及交易監察，以加強識別可疑申請和「傀儡戶口」活動。此舉有效強化數碼身份認證及客戶盡職審查流程，提升金融體系的整體防詐騙能力。

Another key advancement in 2025 was the deeper integration of Scameter data into banking and financial sector. Banks and financial institutions have integrated high risk indicators identified by Scameter—such as phone numbers, emails, IP addresses, and receiving accounts—into customer onboarding and transaction monitoring processes to enhance the identification of suspicious applications and "stooge account" activities. This effectively strengthens digital identity verification and customer due diligence procedures, thereby boosting the overall anti-fraud capability of the financial system.

透過 AI+ 升級及與金融界日益緊密的協作，「防騙視伏App」已由一個查詢工具進化為一個可擴展的跨界早期預警與風險緩控平台，進一步鞏固香港的網絡安全及反詐騙策略。

With the AI+ upgrade and increasingly close collaboration with financial institutions, Scameter+ has evolved from a public enquiry tool into a scalable, cross-sector early-warning and risk-mitigation platform, further bolstering Hong Kong's cybersecurity and anti-deception strategy.

## 網絡安全行動中心聯盟
## Security Operation Centre Alliance (SOCA)

2024年下旬，網罪科正式成立名為「網絡安全行動中心聯盟」(SOCA) 的核心網絡威脅情報交流平台，串聯香港大型及重要基礎設施。「網絡安全行動中心聯盟」成員來自不同界別，包括但不限於航空運輸、銀行與金融服務、通訊、能源、政府、醫療保健服務、陸路運輸、海事、公共事業、廣播服務等。透過分析來自各個成員提供的情報，網罪科得以全面了解針對香港的網絡安全威脅，並適時發出預警及作出即時應對。

In late 2024, CSTCB officially established the Security Operation Centre Alliance (SOCA), a core cyber threat intelligence sharing platform that connects major and critical infrastructure operators in Hong Kong. Members of SOCA come from various industries, including but not limited to air transport, banking & financial services, communications, energy, government, healthcare services, land transport, maritime, public utilities, and broadcasting services. By analysing intelligence provided by its members, CSTCB gains a comprehensive understanding of cybersecurity threats targeting Hong Kong, enabling timely warnings and immediate responses.

2025年，成員已在「網絡安全行動中心聯盟」平台上傳了超過150萬項網絡威脅情報，讓網罪科更快識別威脅類型及攻擊鏈，從而及早發布預警，協助本地機構加強監察、修補漏洞及調整網絡安全策略。同時，跨行業情報共享亦能提升事故應變協調，減少大型事故風險，構建更具韌性的網絡安全生態。這些資料亦有助公私營機構提高警覺，促進制定長遠防護政策，全面改善香港的數碼安全環境、提升香港整體網絡防禦水平，並增強社會整體防護能力。網罪科將持續融合更多創新技術到「網絡安全行動中心聯盟」平台，並積極深化香港網絡安全生態的發展。

In 2025, SOCA members uploaded over 1.5 million pieces of cyber threat intelligence to the platform, allowing CSTCB to rapidly identify threat types and attack chains. This early detection capability facilitates the issuance of timely warnings to organisations or sectors under threat, helping local organisations strengthen monitoring, patch vulnerabilities, and adjust cybersecurity strategies. Moreover, cross-sector intelligence sharing enhances incident response coordination, reducing the risk of large-scale incidents and fostering a more resilient cybersecurity ecosystem. These insights also help public and private sector organisations heighten vigilance, promote the formulation of long-term protection policies, and comprehensively strengthen Hong Kong's digital security environment, its overall cyber defence capabilities, and societal resilience. CSTCB will continue to integrate innovative technologies into the SOCA platform and actively advance the development of Hong Kong's cybersecurity ecosystem.

# 常用詞彙 Glossary

| 簡稱Abbreviations | English | 中文 |
|---|---|---|
| AI | Artificial Intelligence | 人工智能 |
| AML/CTF | Anti-Money Laundering and Counter-Financing of Terrorism | 打擊洗錢及恐怖分子資金籌集 |
| API | Application Program Interface | 應用程式界面 |
| APT | Advanced Persistent Threat | 進階持續性攻擊 |
| C2 | Command & Control | 命令與控制 |
| CADET | Cyber Attack and Defence Elite Training cum Tournament | 網絡攻防精英培訓暨攻防大賽 |
| CSATF | Cyber Security Action Task Force | 網絡安全特別行動小組 |
| CSPA | Cyber Security Professional Awards | 網絡安全精英嘉許計劃 |
| CSTCB | Cyber Security and Technology Crime Bureau | 網絡安全及科技罪案調查科 |
| CyberEx | Cybercrime Expert Group | 網絡罪案專家組 |
| DDoS | Distributed Denial-of-Service | 分散式阻斷服務 |
| DeFi | Decentralised Finance | 去中心化金融 |
| DFEG | Digital Forensics Expert Group | 數碼法理鑑證專家小組 |
| DoS | Denial-of-Service | 阻斷服務 |
| DPO | Digital Policy Office | 數字政策辦公室 |
| EDR | Endpoint Detection and Response | 端點偵測和回應 |
| HKCERT | Hong Kong Computer Emergency Response Team | 香港網絡安全事故協調中心 |
| HKIRC | Hong Kong Internet Registration Corporation Limited | 香港互聯網註冊管理有限公司 |
| HKPF | Hong Kong Police Force | 香港警務處 |
| HKSARG | Government of the Hong Kong Special Administrative Region | 香港特別行政區政府 |
| IDFC | International Digital Forensics Challenge | 國際數碼鑑證挑戰賽 |
| IoT | Internet-of-things | 物聯網 |
| IP | Internet Protocol | 互聯網規約 |
| IT | Information Technology | 資訊科技 |
| LCGE | Legislative Council General Election | 立法會換屆選舉 |
| LLM | Large-Language-Model | 大型語言模型 |
| MFA | Multi-factor authentication | 多重認證 |
| M.O. | Modus Operandi | 犯案手法 |
| NAS | Network Attached Storage | 網絡儲存設備 |
| NG | National Games | 全國運動會 |
| OFCA | Office of the Communications Authority | 通訊事務管理局辦公室 |
| PCPD | Privacy Commissioner of Personal Data | 個人資料私隱專員 |
| POS | Point-of-sale | 銷售點 |
| RaaS | Ransomware-as-a-service | 勒索軟件即服務 |
| RCE | Remote Code Execution | 遠端執行程式碼 |
| RDP | Remote Desktop Protocol | 遠端桌面協定 |
| SaaS | Software-as-a-service | 軟件即服務 |
| SME | Small and medium enterprise | 中小型企業 |
| SOCA | Security Operation Centre Alliance | 網絡安全行動中心聯盟 |
| SPAP | Smart Policing Advisory Panel | 智慧警政顧問小組 |
| SQL | Structured query language | 結構化查詢語言 |
| SSH | Secure Shell Protocol | 安全外殼協議 |
| TTPs | Tactics, techniques, and procedures | 策略、技術和程序 |
| UAT | User Acceptance Test | 用戶驗收測試 |
| VAIT | Virtual Asset Intelligence Taskforce | 虛擬資產情報工作組 |
| VPN | Virtual Private Network | 虛擬私有網絡 |
| XDR | Extended Detection and Response | 延伸偵測和回應 |

# 方法 Methodology

網罪科透過案件調查、與合作夥伴共享情報，以及其他可靠來源，收集和分析網絡威脅情報，從而更全面了解全球及香港的網絡安全形勢。

CSTCB collects and analyses cyber threat intelligence from multiple sources, including case investigations, intelligence sharing with working partners, and other reliable channels. This multi-source approach enables a comprehensive overview of the cybersecurity landscape, both globally and in Hong Kong.

本報告所呈列的數據來自多個可信來源及業界意見，但並非旨在全面涵蓋或代表全球所有網絡安全趨勢。報告中的結論和觀察旨在提供對新興網絡威脅模式和風險的概括性參考，而非作為權威性或全面性的分析依據。

The data presented in this report are drawn from a selection of credible sources and industry insights, though they are not exhaustive or representative of all global cybersecurity trends. The conclusions and observations herein aim to provide a general reference for understanding emerging patterns and risks, rather than serving as a definitive or comprehensive analysis.