



HKCERT

Keeping Pace with Emerging Trends in Cybersecurity

Hong Kong Computer Emergency Response Team (HKCERT)
Coordination Centre 香港電腦保安事故協調中心



About HKCERT

2001

Founded

100%

Funded by
Government

7 x 24

Operation

7,051

Incidents Handled

330+

Security Advisories

2M+

People Reached

530+

People Trained

100%

of cases resolved
within 5 working days

International

Local

Exchange Incidents
and Information

HKCERT as a Hub

Coordinate incidents
and publish alerts

Global
Researchers

FIRST
Improving Security Together

Global CERT Forum

APNIC

DOT ASIA
ORGANISATION

APCERT
Asia Pacific Computer Emergency Response Team

Regional CERT
Forum



HKCERT



GovCERT.HK



Internet
Infrastructure



Regulators



Enterprises



Universities &
Researchers



IT & Security
Vendors

Service and Support by HKCERT



Monitoring

- **Collect and Analyse Attack Patterns**
- **Provide Early Information Security Alerts**



Education and Technical Advice

- **24-hours Free Incident Report Hotline (8105-6060)**
- **Organise Free Seminars and Briefings**
- **Collaborate with Local Industry, Government Agencies, and Global CERTs**



Research and Insights

- **Offer Best Practice and Guideline**
- **Provide Online Cyber Security Self-Assessment Tool**

5 Key Information Security Risks in 2023



1

Identity/Credential Theft 身份 / 憑證盜用

2

Attacks Utilising A.I. 利用人工智能的攻擊

3

Crime as a Service 網絡犯罪服務

4

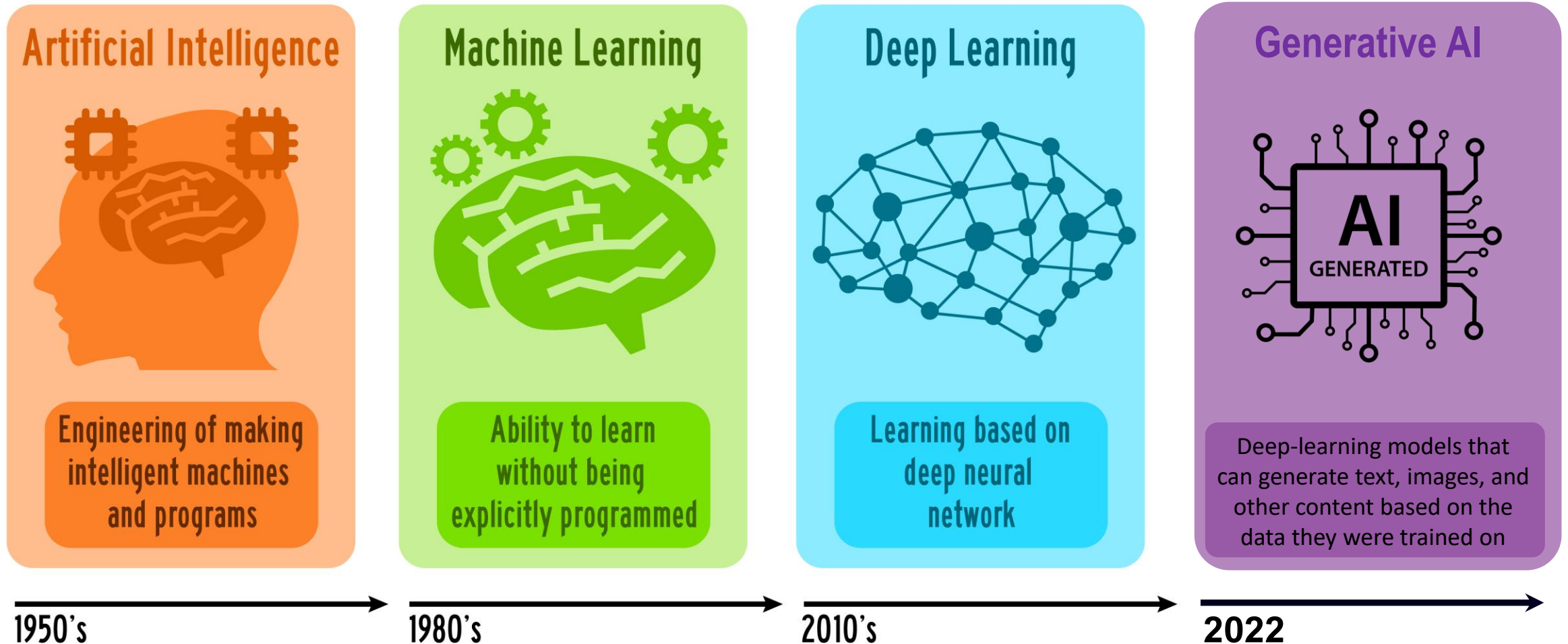
Cyber Attacks Targeting Web 3.0
針對 Web 3.0 的攻擊

5

Attacks Arisen from Widespread Application of IoT
IoT 廣泛應用引發的 攻擊

(In no particular order 排名不分先後)

Evolution of Artificial Intelligence



2.19256

AI

ARTIFICIAL
INTELLIGENCE

**AI in
Cybersecurity
Friend or
Foe?**

0001



AI as a friend in Cybersecurity

- **Analyse** – Analyse patterns and abnormalities (e.g. security log, network activities, etc)
- **Detect** – Analyse the behavior of files and programs, allowing it to detect new and unknown malware variants
- **Response** – Automate remediation and isolation



Deepfake

**Adversarial
Attack**

Phishing

**AI powered
malware**

Good luck speed cameras.

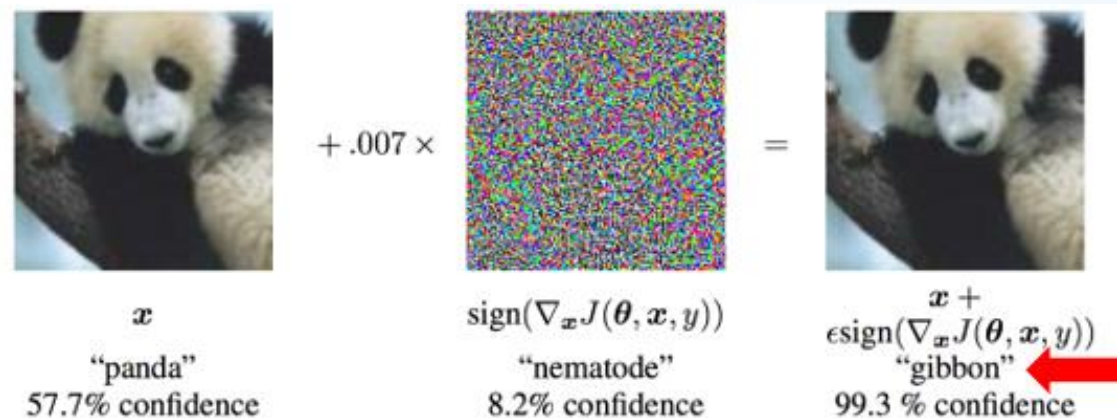
Adversarial
Attack



Adversarial Attack

Evasion Attacks (one-off impact)

- Directs the model to **misclassify** a certain target class of data to get desired labels of the attacker by **introducing meaningless inputs (i.e. noise)**.
- This kind of input tampering could be unnoticeable but remains greatly effective in **fooling the learning model**.
- A conference [paper](#) from Google demonstrated the concept and potential result below: The panda has been added with suitable noise and the model misclassified it as a gibbon.

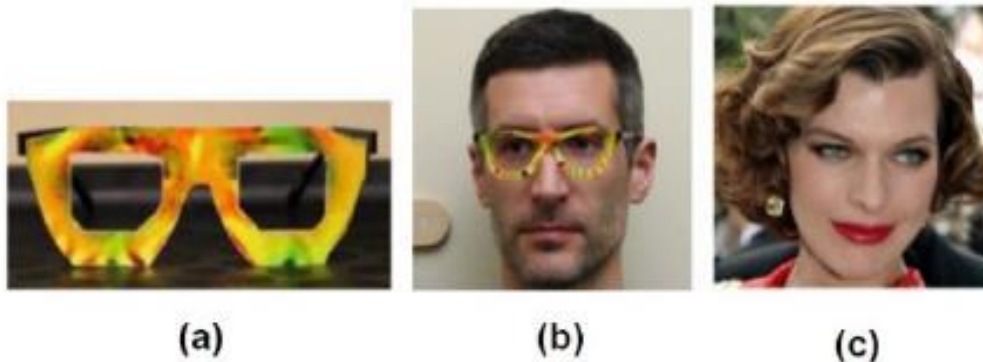
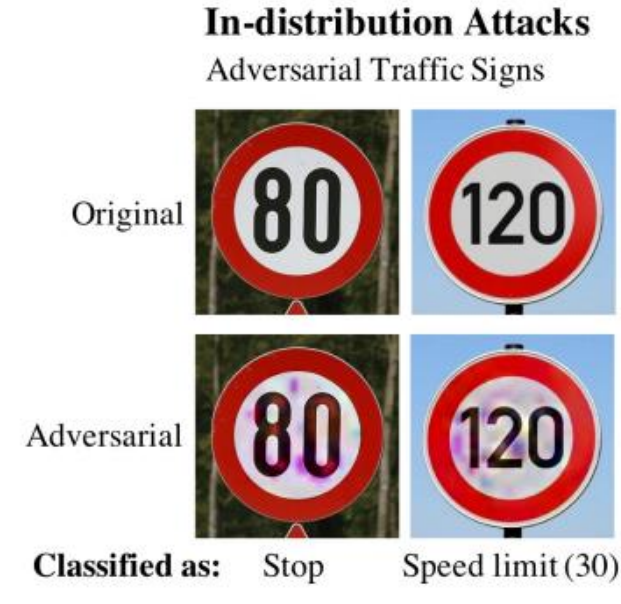


Adversarial Attack

Evasion Attacks (one-off impact)

- Traffic Signs

[Deceiving Autonomous Cars with Toxic Signs](#)



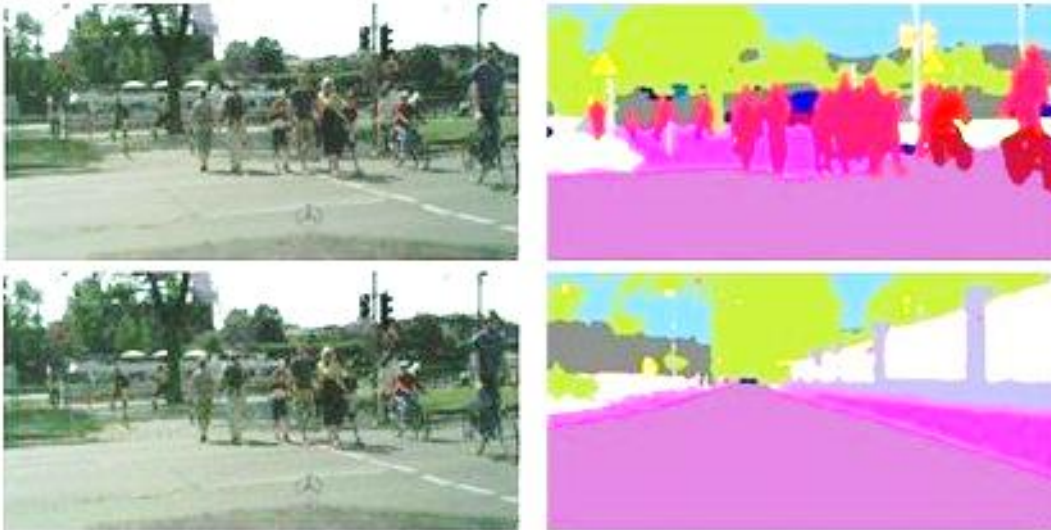
The eyeglass frames (a) were used by Lujo Bauer (b) to impersonate Milla Jovovich (c)

[Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition](#)

Adversarial Attack

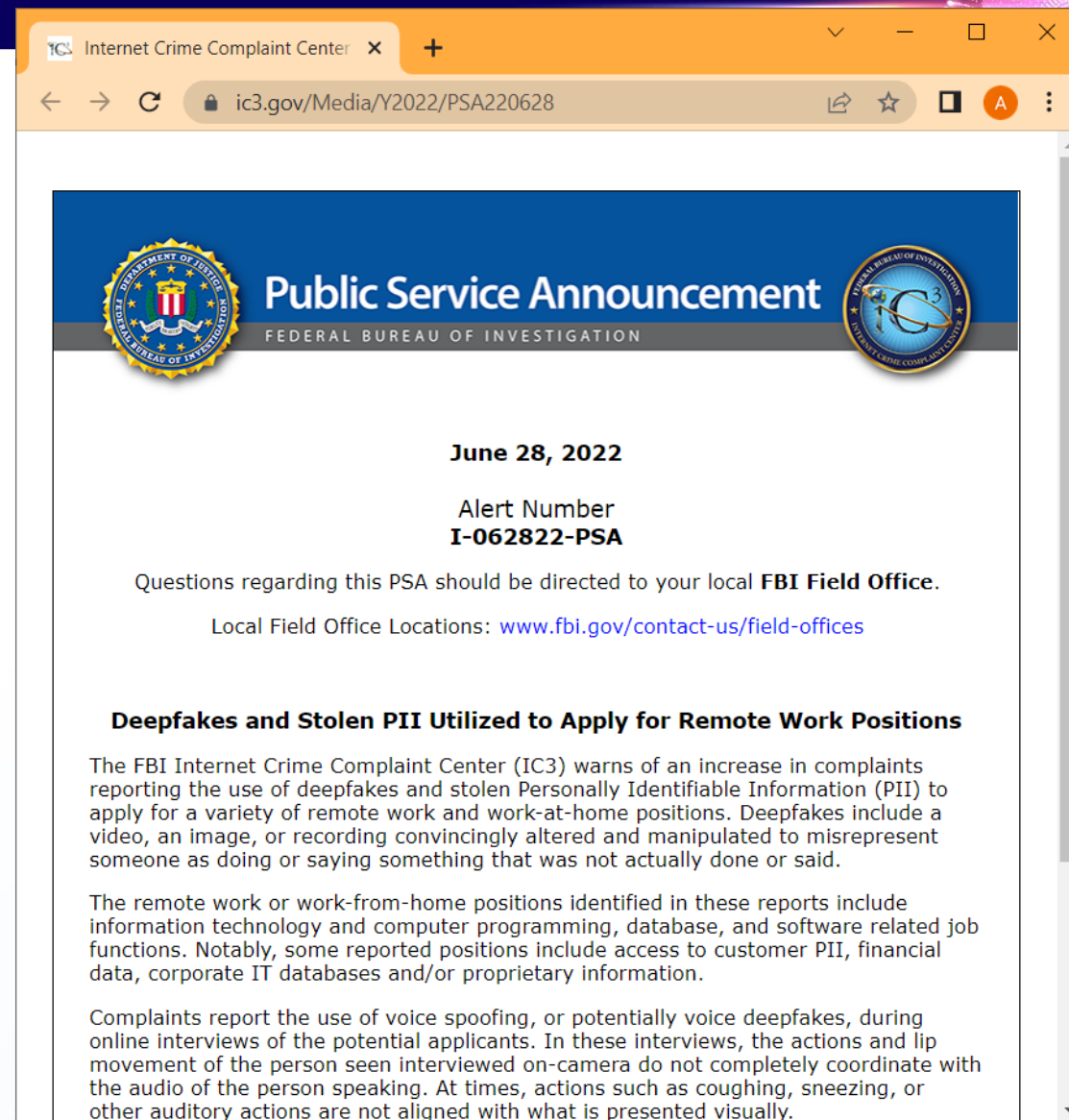
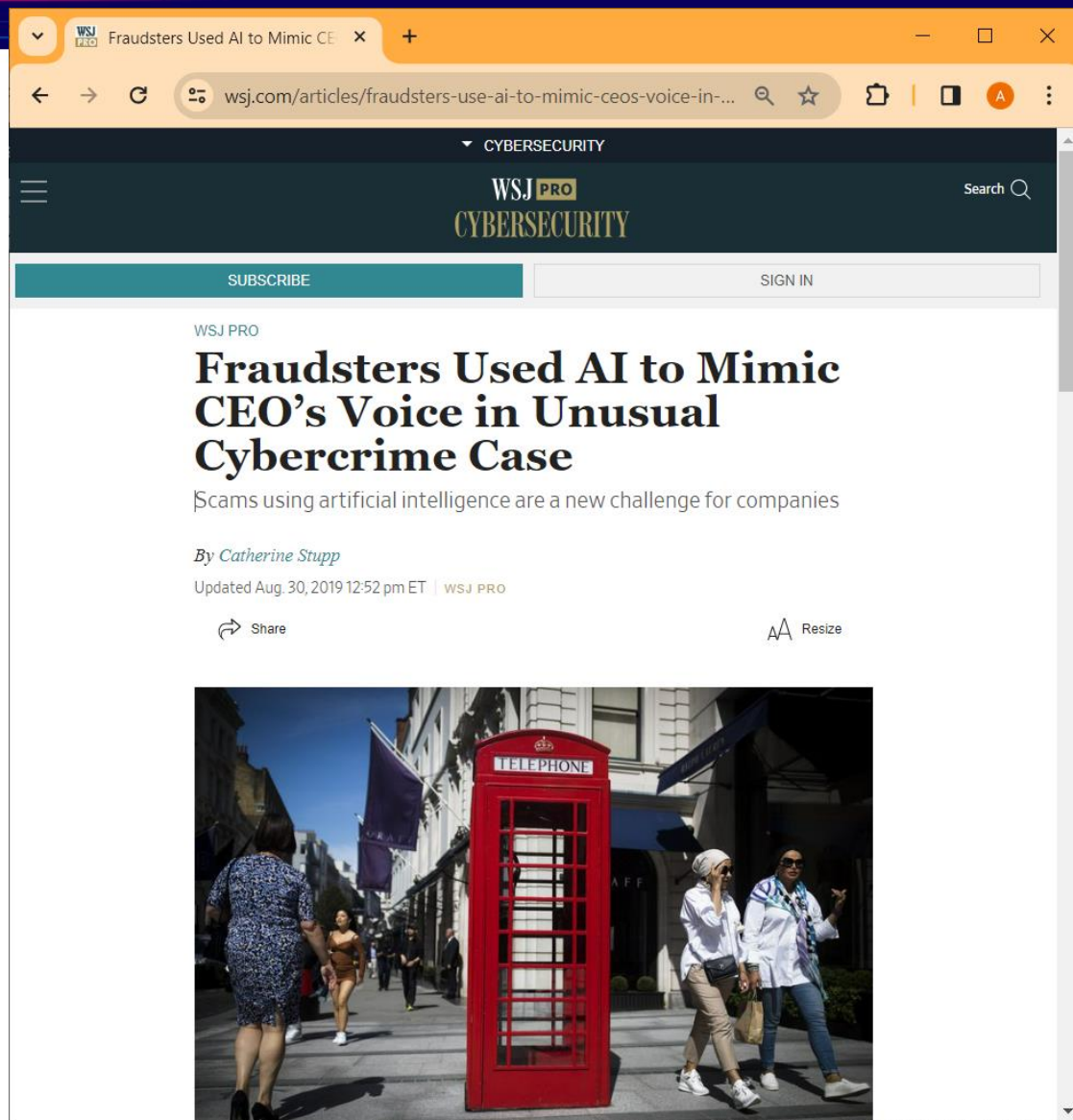
Poisoning Attacks (substantial impact)

- Introduces misleading training data to make the model misclassify. The attacker **compromises the AI model in the learning stage** and inject manipulated data into it.
- The aim is to **corrupt the model** and produce the output desired by the attacker in the future. It has a serious impact as it can affect the model substantially if not discovered

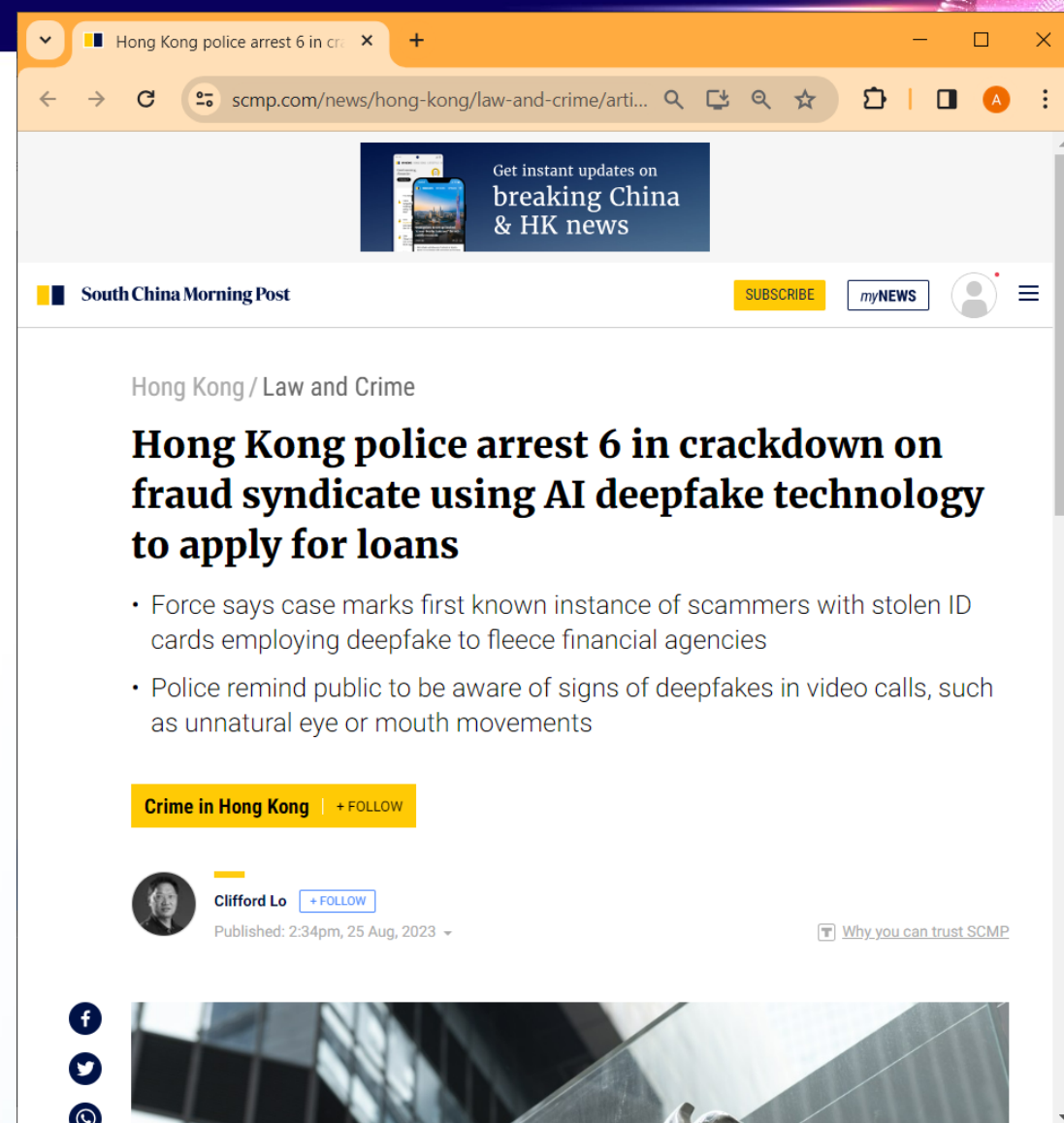
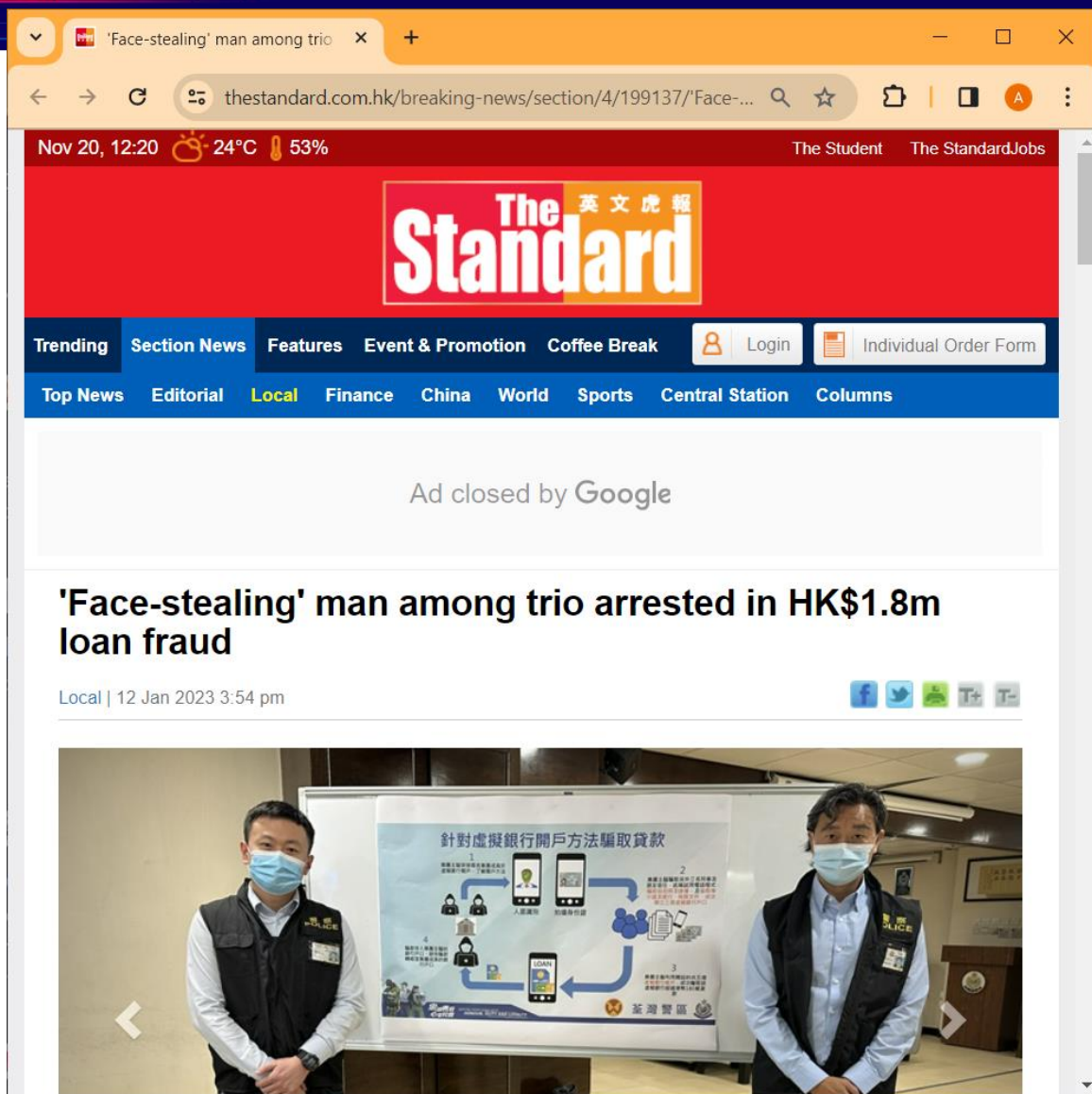


- An experiment conducted by researchers in Bosch AI demonstrated that it is possible to insert adversarial perturbations into street views so that the image segmentation model **cannot detect pedestrians**.
- If **autopilot systems** are being attacked this way, the car may crash into pedestrians and cause great casualties.

DeepFake



DeepFake



DeepFake



Tips to Detect DeepFake



Typical Phishing Email

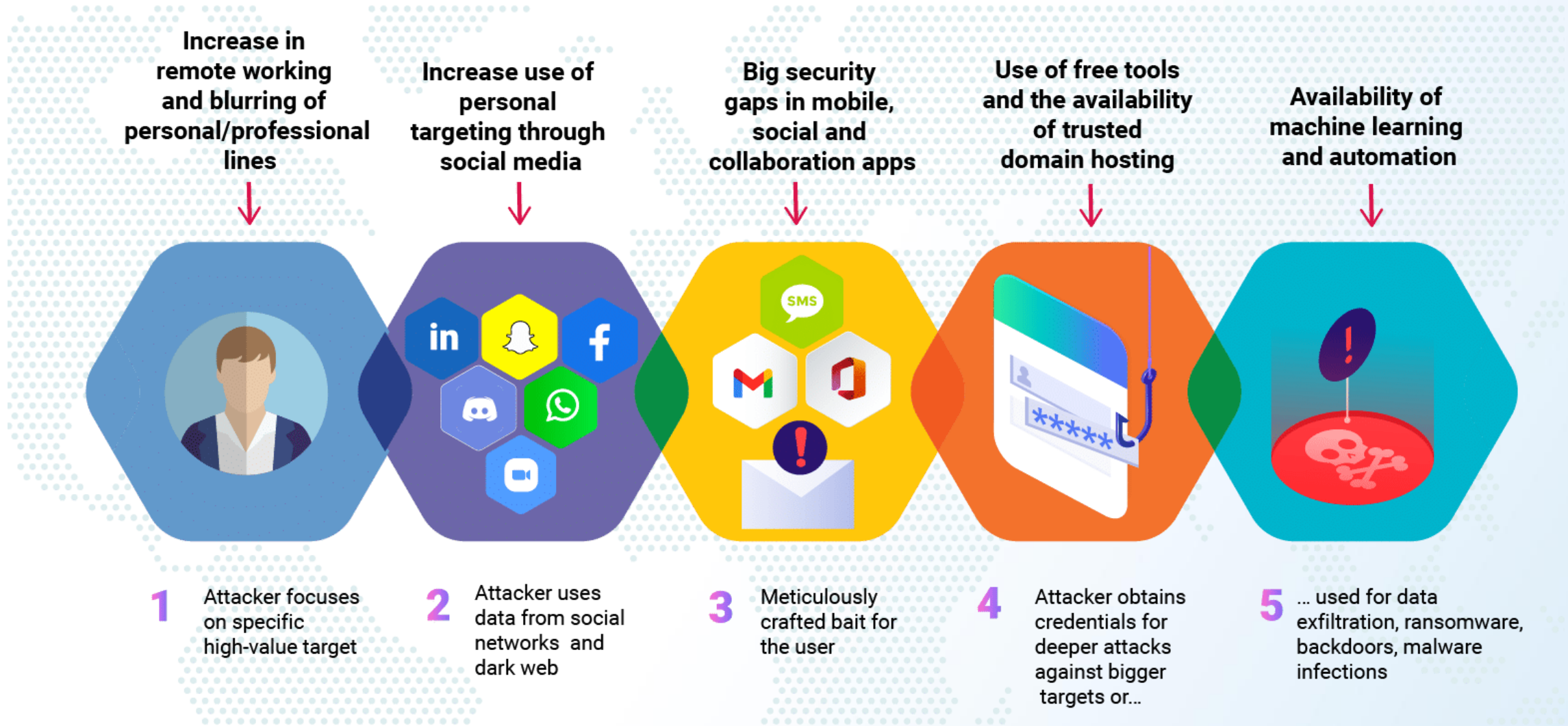


- 1 Grammatical error
- 2 Unrealistic reward
- 3 Unusual request

Congretulations! You have won a \$10000 credit reward. Please login your bank a/c www.futurebambk.top to claim your reward immediately. Otherwise, your bank a/c will be suspended.

- 4 Misleading link
- 5 Urgent tone

More Complicated Phishing



- Less effort and programming knowledge required for developing Malware



In contrast with ChatGPT or Google's Bard, WormGPT doesn't have any guardrails to stop it from responding to malicious requests

Recommendations





**Spending Million Dollar on
Cyber Defense Solutions**

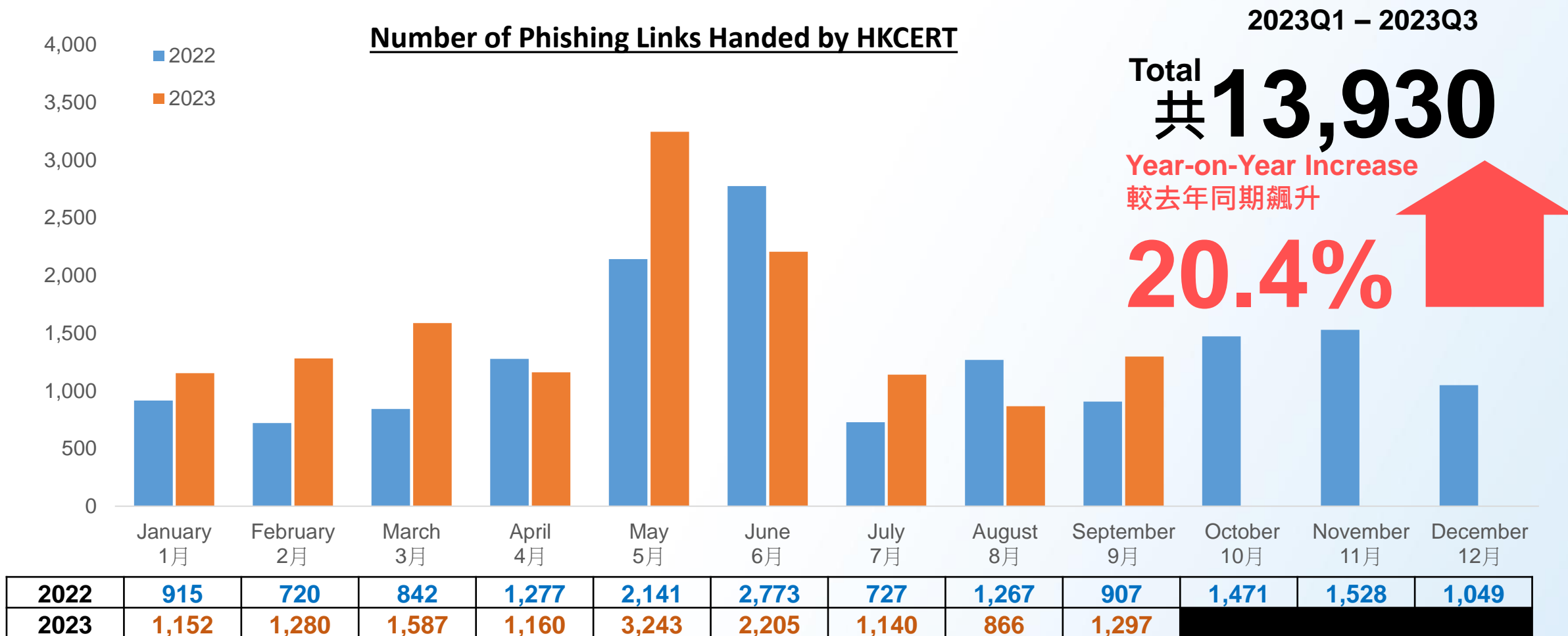
The common cyber attacks
are not AI related, instead,
over 50% is phishing



**User Click a Phishing Link and Input
his Username and Password**

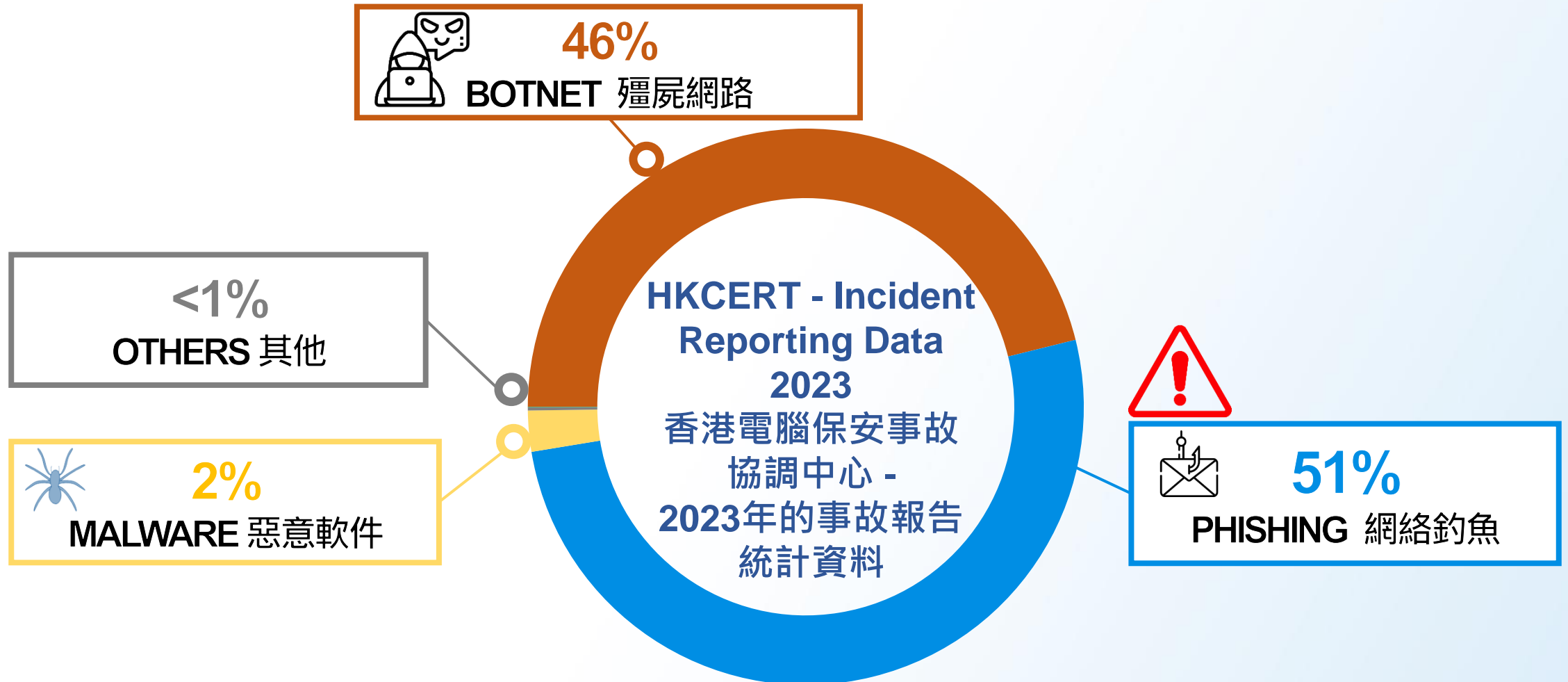
HKCERT - Incidents Reporting Data (as of September 2023)

香港電腦保安事故協調中心 - 事故報告統計資料 (截至2023年9月)



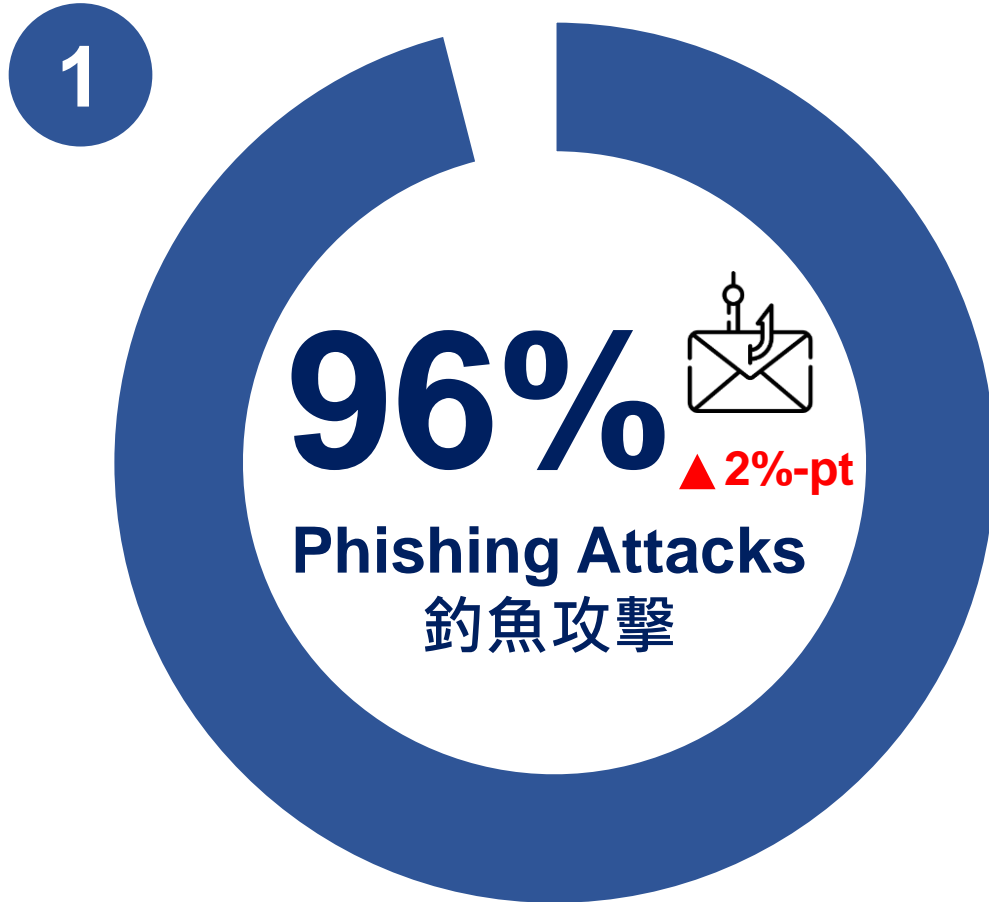
HKCERT - Incident Reporting Data 2023 (as of September 2023)

香港電腦保安事故協調中心 - 2023年的事故報告統計資料 (截至2023年9月)



Top 5 Cyber Security Attacks Encountered in the Past 12 Months

過去12個月面對的五大網絡安全攻擊



- 2 **17%** ▲ 1%-pt  **Other Malware including Botnet**
其他惡意軟件 包括殭屍網絡
- 3 **15%**  **Ransomware**
勒索軟件
- 4 **14%** ▲ 3%-pt  **Web Server & App Attacks**
針對網絡服務器/ 應用程式的攻擊
- 5 **11%** (New)  **Hacking targeting corporate service accounts**
攻擊企業的網上服務帳戶

▲ ▼ Changes compared with 2022
比較2022年的轉變

Phishing Attacks 釣魚攻擊



Base: Those who encountered Cyber Security Attacks in P12M
基數：在過去12個月內有遇到網絡安全攻擊的企業

▲ ▼ Changes compared with 2022
比較2022年的轉變

The server has infected by ransomware

A scene from the movie Inception showing Leonardo DiCaprio and Matt Damon on the deck of a ship. DiCaprio is in the foreground, looking slightly to the right with a serious expression. Damon is behind him, looking towards the camera with a slight smile. The background shows the ocean and a cloudy sky.

Where is backup?

A close-up shot of Leonardo DiCaprio and Matt Damon from the same scene. DiCaprio is in the foreground, looking off-camera with a serious expression. Damon is behind him, looking towards the camera.

On the server

Backup Rule: 3-2-1



Three different
copies of data



Two different media



One offsite copy

veeam



Of which is:
offline air-gapped
or immutable



No errors after
automated backup
testing &
recoverability
verification

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

A man and a woman are seated at a table, facing each other. The man, on the left, is seen from the side, wearing a white shirt. The woman, on the right, has long dark hair and is wearing a white long-sleeved shirt. She has a skeptical or questioning expression on her face, with her hands clasped near her chin. The background is a bright, out-of-focus interior with white curtains.

Learn from your wife / girl friend ...

**Zero Trust Principle
Never Trust,
Always Verify**

HKCERT Information Security Alert Service

To stay vigilant against **information security risks**, please subscribe or follow:

1. Free Security Bulletin and Monthly Newsletter



2. Free SMS Alert



3. HKCERT's Social Media Platforms (e.g., Facebook, LinkedIn and YouTube)



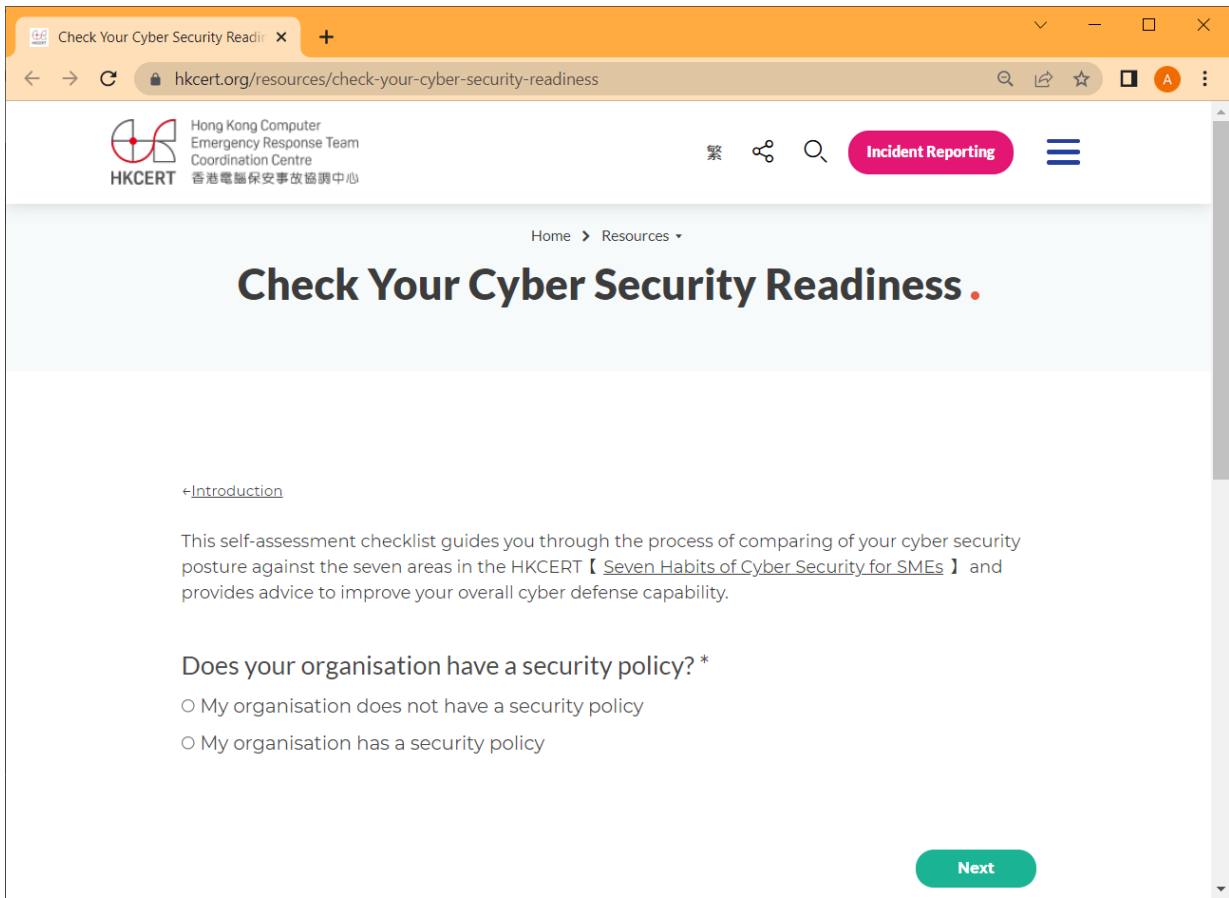
Take Action Now!

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

SUBSCRIBE



Online Self Assessment & Incident Response Guideline for SMEs



The screenshot shows a web browser window with the URL hkcert.org/resources/check-your-cyber-security-readiness. The page header includes the HKCERT logo and navigation links. The main heading is "Check Your Cyber Security Readiness." Below this, there is an "Introduction" section stating: "This self-assessment checklist guides you through the process of comparing of your cyber security posture against the seven areas in the HKCERT [[Seven Habits of Cyber Security for SMEs](#)] and provides advice to improve your overall cyber defense capability." A question is posed: "Does your organisation have a security policy? *". Two radio button options are provided: "My organisation does not have a security policy" and "My organisation has a security policy". A green "Next" button is located at the bottom right of the form.



Phishing Exercise & Cyber Security Awareness Training

網絡釣魚演習 及 網絡安全培訓

Awareness Training

網絡安全培訓

- Encourage lasting behavioural change by providing employees with **engaging security awareness training** designed to capture their attention and reinforce their security habits
鼓勵員工透過**安全意識培訓**來實現持久的行為改變，提高員工的注意力並強化安全習慣

Targeted Learning

針對性學習

- Targeted microlearning for any failed attempts** to boost employees' threat identification and reporting skills
未成功的嘗試會觸發針對性的微學習，以改善未來威脅的識別和報告



<https://www.hkpc.org/zh-HK/our-services/digital-transformation/cyber-security/phishing-defence-services>

Sophisticated Phishing Attacks Simulation

模擬複雜的釣魚攻擊

- Simulations to replicate common scam tactics** like domain spoofing and typosquatting
模擬常見詐騙手段，如域名偽造和網址釣魚

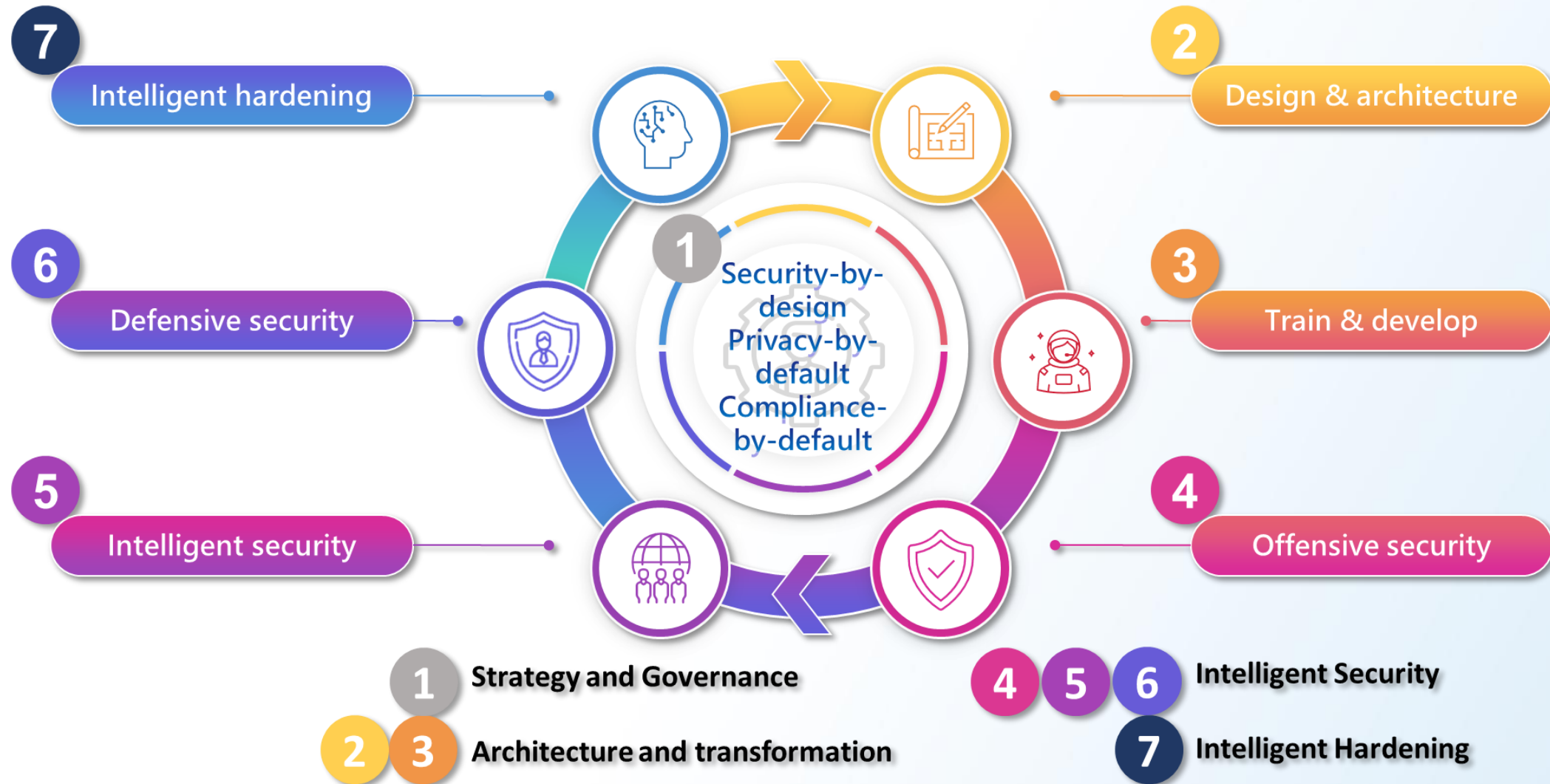
Reports and Assessments

報告與評估

- Response tracking and automated report functions** simplify the generation of charts and compliance documents
自動化報告和追蹤功能大幅簡化了圖表和合規文件生成
- Data-driven** security training programmes
基於數據的安全培訓計劃



HKPC Cybersecurity Framework



Cyber Security Training Courses

Over 20 different training courses are available for matching different market needs to improve people cyber security capability in areas such as Cyber Security, DevSecOps, Red Blue Team, Secure Big Data, ISO, Mobile Security and more!

(ISC)² - PROFESSIONAL SECURITY CERTIFICATION

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

KUNGFU SERIES

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

EC-COUNCIL - ETHICAL HACKER SERIES

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

CHECK POINT SERIES (COMING SOON)

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

ISO SERIES

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

MOBILE SECURITY SERIES

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

CLOUD SERIES & SECURE CODING

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



To know more



Thank you