

Digital Policy Office introduces initiatives to promote cybersecurity in 2025 (with photos)

The Digital Policy Office (DPO) introduced the key initiatives for promoting cybersecurity this year at the 2025 Cybersecurity Initiatives Briefing today (March 27). Representatives from the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force, the Hong Kong Internet Registration Corporation (HKIRC) and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) also shared the latest trends in cybercrime and a series of measures to strengthen capability of small and medium enterprises (SMEs) on cybersecurity defence.

The Commissioner for Digital Policy, Mr Tony Wong, said that as smart technologies become increasingly prevalent, enterprises are relying more on information systems for their operations. This growing dependence necessitates a heightened focus on cybersecurity to strengthen defences against emerging threats to avoid reputational and financial losses. In introducing the cybersecurity initiatives co-ordinated by the DPO this year, Mr Wong said in addition to the ongoing collaborations with the CSTCB, HKIRC, HKCERT and various stakeholders to provide local enterprises (in particular SMEs) with information security incident response support, issue security threat alerts, offer preventive guidelines and security education, and continue to strengthen the Hong Kong Cybersecurity Attack and Defence Drill, the DPO will also co-ordinate with the HKIRC and HKCERT to launch two new initiatives, the Cybersec One Programme and the Cybersecurity Vendor Connect Programme, to further raise SMEs' awareness of information security and support them in addressing cybersecurity risks.

The Chief Superintendent of the CSTCB, Mr Lam Cheuk-ho, announced the latest technology crime figures at the briefing. A total of 33 903 cases were recorded in 2024, representing a slight decrease of 0.6 per cent when compared to 2023. The data shows that while the majority of technology crimes are Internet-related deception, some also involve cyberattacks against enterprises, including system intrusions, distributed denial of service (DDoS) and ransomware. Mr Lam emphasised that in the face of rampant cybercrimes, the Police will not only continue to strengthen law enforcement but also adopt a multipronged approach to promote Hong Kong's cybersecurity, including assisting the Government in taking forward the legislation, raising public awareness and strengthening public-private collaborations.

At the briefing, the Chief Executive Officer of the HKIRC, Mr Wilson Wong, introduced some common website vulnerabilities. He noted that although patching vulnerabilities promptly can reduce losses, once a brand's reputation is damaged, regaining customer confidence can become very difficult. He called on organisations to register for the services of the Cybersec One Programme, which provides free risk assessments, vulnerability identification, and staff training to enhance information security of

organisations. The General Manager of Digital Transformation Division, Hong Kong Productivity Council (HKPC) and spokesperson of the HKCERT, Mr Alex Chan, also pointed out that SMEs are generally facing challenges such as insufficient cybersecurity expertise and budget and resource constraints. He added that the HKCERT will launch the Cybersecurity Vendor Connect Programme to help organisations find suitable and cost-effective cybersecurity solutions.

In conclusion, Mr Tony Wong emphasised that cybersecurity is not just an issue to individual sectors; it also affects the health and stability of Hong Kong's overall digital economy and social development. It is a task that all sectors and the public need to pay attention to and participate in. The DPO will continue to launch a variety of activities and provide training to enhance Hong Kong's overall capabilities to tackle risks in cybersecurity, and he appealed for media support in jointly disseminating important cybersecurity messages to the general public.

