

Contents

Contents.....	1
HKMA warns about fake Hang Seng Bank Webpage.....	1
Hong Kong Cybercrime Increases Again; Privacy Under Attack.....	1

HKMA warns about fake Hang Seng Bank Webpage

[<web-link for this article>](#)

The Hong Kong Monetary Authority (HKMA) has warned that the webpage "http://hsplbk.com/bank.hangseng.com/1/2/personal/private-banking/private-banking.html" is a fraudulent copy of the official website of Hang Seng Bank, Limited (HSB). The page is unavailable at the time of writing and the Police are investigating.

Please contact HSB at 2822 0228 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012 if you have used the site.

The domain hsplbk.com was registered in March 2014 and the site was hosted by UK company Fasthosts Internet Ltd. According to Google, the domain hosted at least seven other fake HSB pages, and no trace of innocent pages were found in Google or the [Internet Archive](#). This suggests that the criminals deviated from common criminal practice of hosting their fraudulent pages on compromised legitimate websites, and choose to register the domain legally solely for this fake HSB site. If that is the case, the site might have been operating undetected for ten months.

More Information

- [Fraudulent website: http://hsplbk.com/bank.hangseng.com/1/2/personal/private-banking/private-banking.html](http://hsplbk.com/bank.hangseng.com/1/2/personal/private-banking/private-banking.html)

Hong Kong Cybercrime Increases Again; Privacy Under Attack

[<web-link for this article>](#)

Despite overall crime figures hitting a 41 year low, Commissioner of Police Mr Tsang Wai-hung reported in his 2014 crime review that cybercrime has risen for the third year in a row. In a separate report, Mr Allan Chiang, Privacy Commissioner for Personal Data, said that 2014 saw a two-fold increase in privacy complaints related to use of Information and Communications Technologies.

1,239 cases involved deception on social media, a 375% increase for around \$70 million losses, mostly involving fraudsters illegally logging in to an instant messaging account,

contacting friends of the user, asking them to purchase Game Cards and send the serial number and PIN. The fraudsters then sold the credentials.

Online business fraud rose by 64% to 2375 cases and \$48 million losses. Most cases involved e-auction and online shopping.

'Naked chat' blackmail cases rose 34% to 638 cases, with losses of \$2.3 million. The highest amount lost in a single case was around \$110,000.

In the Privacy Commissioner's report, there was a sharp increase of 44% in internet related enquiries to 611 cases in 2014. They were mainly concerned with cyber-profiling, excessive collection of personal data and cyber-bullying.

More Information

- [Hong Kong Police Force Press Releases](#)
- [‘Sense of lawlessness’ spreading in Hong Kong says police commissioner](#)
- [Year 2014 Saw a Two-fold Increase in Privacy Complaints Related to Use of Information and Communications Technologies](#)
- [Hong Kong Cybercrime on the Rise](#)
- [Hong Kong Cybercrime Continues to Soar](#)
- [Occupy Central protests blamed for increase of cyberbullying in Hong Kong](#)



Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
<http://www.yuikee.com.hk/>

<http://www.yuikee.com.hk/>

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

E-Learning

- Content & Curriculum Development
- Training

Security

*Your
Peace of Mind
Is Our
Commitment*

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Education

- Project Development & Management
- Educational Software Distribution

<http://education.yuikee.com.hk/>