

Beware of Phishing



INFOSEC
Office of the Government
Chief Information Officer



Hong Kong Computer
Emergency Response Team
Coordination Centre



Hong Kong Police Force

For details, please visit the InfoSec website at:
www.infosec.gov.hk

Do not open emails and messages of dubious origin or unrelated to your business



Do not visit suspicious websites and do not click on links or download attachments from them

Contact the sender to confirm the authenticity, if you are in doubt with the received email or message



Enter the website address directly into a web browser or use a bookmark

Avoid sending personal, financial or sensitive information by email

Review the account status (e.g. last login time) regularly and change the password as soon as suspicious activities are detected



Adopt strong authentication mechanism if available

URL bar containing both the "https" and the green padlock icon is not necessarily a sign of a trusted website

Enable security features such as anti-phishing and malware protection and keep anti-malware program and its signatures up-to-date

Report any phishing matters to the related organisation or the Police for investigation

Anti-Scam
Helpline
18222