Security Measures Adopted by China Mobile Hong Kong Company Limited

中國移動香港有限公司採取一系列安全措施保障數據安全

中國移動香港有限公司
China Mobile Hong Kong Co. Ltd.

Mr. Sean Lee
Director & Chief Executive Officer
China Mobile Hong Kong Company Limited
李帆風先生
董事兼行政總裁
中國移動香港有限公司

Interviewed by : Dr. Hubert Chan
採訪者：陳重義博士

China Mobile Hong Kong Company Limited ("CMHK") has been a leading mobile network operator in Hong Kong for years. In the past two decades, with the rapid breakthroughs in technology, CMHK has been providing many outstanding services to Hong Kong citizens.

According to CMHK, they launched the world's first converged commercial LTE network in 2012 and successfully introduced 4.5G mobile network in November 2016. CMHK also states that they are the first mobile operator to provide 4G network coverage in 16 tunnels throughout Hong Kong in 2016. CMHK has reached some key milestones in 2017. They are Hong Kong's first mobile operator to cloudify its core network in February; the world's first operator to launch commercial 2.3GHz TDD Massive MIMO technology in August; and the first operator to launch NB-IoT commercial service in September. Without technology advancement, it would not be possible of CMHK to deliver such high-quality services. CMHK was awarded the "Trial Permit for 5G Test" (5G技術測試許可證) by the Office of Communications Authority (OFCA) and has been conducting lab tests continuously with 5G commercial equipment within the assigned 5G trial spectrum since March 2018. CMHK is committed to acquiring 5G technologies and application experiences to build a solid foundation for the leading technology development.

CMHK's Approach to Data Security

Data security is one of the major concerns in the digital world. To address internal security, China Mobile Hong Kong has set up a department which is responsible and accountable for IT security administration. This department works with the legal department to provide timely updates on cybercrime trends and offer continuous trainings that focuses on enhancing cybersecurity for internal staff. CMHK provides "on-demand IT security announcement"

中國移動香港有限公司（CMHK）多年來一直是香港領先的流動網絡供應商。近二十年來，CMHK善用尖端科技，一直為香港市民提供優越服務。

據CMHK表示，他們於2012年推出了全球首個融合LTE網絡服務，並於2016年11月成功推出4.5G流動網絡。2016年，CMHK更是首家在全港16條隧道提供全4G網絡覆蓋的流動網絡供應商。2017年，CMHK更達到幾項關鍵的重要里程。於2月，成為全港第一家將其核心網絡實踐雲端化的流動網絡供應商；於8月，再成為全球第一家推出商用「2.3GHz TDD Massive MIMO」；同年9月，更率先發布全港第一個商用NB-IoT網絡。如果沒有科技上的不斷進步，CMHK不可能提供如此高質量服務。此外，在2018年3月，CMHK更獲得通訊事務管理局（OFCA）發出 5G技術測試許可證，運用5G測試頻譜展開網絡商用設備的實驗室測試。 CMHK致力於5G技術測試和應用經驗，為技術研發之領先及發展打好基礎。

中國移動香港保障數據安全方法

數據安全是數碼世界關注的主要問題之一。針對內部安全問題，中國移動香港成立了專門負責資訊科技安全管理的部門。此部門與法律部緊密合作，持續為內部員工提供網絡安全培訓及提供最新的網絡犯罪趨勢資訊。CMHK更為員工提供「即時資訊科技保安報告」 資訊及面對面的 「資訊保安意識培訓」。課堂式的培訓確保CMHK員工充分了解公司資訊安全政策、程序和應對方法，亦可提高員工對管理資訊責任的意識，以及了解遇到違規問題時衍生的額外風險。舉辦培訓課程旨在確保資訊有效傳遞，包括：每月的入職培訓，每季的部門培訓和按需求的培訓。導師均擁有超過14年的資訊科技系統安全經驗。

service and face-to-face training session, "Information Security Awareness Training", to employees. The classroom-type training ensures CMHK employees have a good understanding of company information security policies, procedures and best practices. The training also raises their awareness of managing their IT responsibility and the additional risks incurred if failing to comply with the rules and regulations. The training sessions are conducted to ensure effective information delivery: once a month for new staff orientation, once every quarter for departmental staff and by on-demand requests. The trainer is provided by their IT Security team with more than 14 years of experience in IT System Security.

Furthermore, data output is separated into three orthogonal categories: 1) mobile data 2) company data 3) corporate data. This is accomplished by implementing safeguards such as firewall, that prevents whoever obtains Email data, for instance, will likely not be able to get their hands on mobile data.

To address security externally, China Mobile adopts the international standards ISO 27001 (information security management system that includes standardized legal and technological protocols), Information security compliance audits, and white hat hacking and penetration testing methodologies to safeguard the security of CMHK's information systems. Customers' data is split into three tiers: basic client info (i.e. phone numbers, passwords), detailed call record, and customer behavior (e.g. spending patterns, data package used). For instance, abnormally long calls (e.g. 7 hours non-stop) are alerted to fraud teams who are responsible for monitoring suspicious activities. These teams monitor scams such as phishing calls, and to keep customers informed of the latest social engineering tactics.

The easiest thing to hack is one's passwords. A.I. robotics technology can go through trials and errors countless times. To counter this, some operators have users receive a text if their accounts were hacked into so they can change their password, and/or go through CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) tests to tease out humans from machines. The former aims to prevent hackers from accessing private data, while the latter ensures that hackers are humans instead of machines. Both measures are required by CMHK, and as of now, no confirmed data breach has occurred to China Mobile.

Tackling Telephone Deception

The Legislative Council Secretariat's research office states that Telephone deception is the second largest category of crime in Hong Kong in 2017, with a share of 13%. Since 2012, telephone deception has been facing an uptrend where the number of deception and fraud cases has surged by 97% in eight years to a peak of 9,353 cases in 2015. Despite the number of telephone deception cases dropped by 66% in the past two years to just

此外，數據輸出劃分成三種主要的類別：1）流動數據 2）公司數據 3）企業數據。這些都受到防火牆等安全措施所保護，確保員工僅可讀取工作範圍的資料，例如負責電郵系統的員工不會同時讀取流動網絡的數據。

對於外部安全問題，中國移動香港採用國際標準 ISO 27001（包括標準化法律和技術協議的訊息安全管理系統）、訊息安全合規審計、白帽黑客攻擊和滲透測試等方法，保障中國移動香港訊息系統的安全。客戶數據分為三個層面：基本客戶信息（例如電話號碼、密碼）、詳細通話記錄和客戶行為（如消費模式、使用的流動數據）。例如，當系統偵測到不尋常的長時間通話（如7小時無間斷），負責監視可疑活動的反欺詐團隊便會收到警報。反欺詐團隊專門監控網絡詐騙行為，如釣魚電話等，並及時警醒客戶最新的欺詐手段。

人工智能技術可以反覆不斷猜度密碼，令密碼成為最容易被攻擊的個人資料。要解決這問題，有些供應商會透過短訊警示用戶帳戶被入侵，並提示用戶修改密碼，或者通過圖片驗證碼測試來辨別人與機器。前者旨在防止駭客竊取私人資料，而後者則可阻擋機器自動化的攻擊。中國移動香港雙管齊下，並嚴格執行，至今未錄得資料外洩個案。

處理電話騙案

立法會秘書處研究小組指出，在2017年，電話詐騙是本港第二大罪案類別，所佔比例為13%。自2012年以來，詐騙或欺騙案件呈上升趨勢，在2015年錄得9,353宗，在八年內飆升了97%。雖然在過去兩年，電話騙案的數目下降了66%，至2017年略低於一千宗，但錄得的財務損失卻回升4%至2.29億港元。

最近，電話騙徒冒名利用CMHK的名義詐騙市民。這些騙徒通常冒認是CMHK的員工，訛稱用戶有欠款，並要求他們轉帳至指定銀行戶口。儘管騙徒撥打大量詐騙電話，幸好大部分市民並沒有墮入騙局，但這種詐騙行為仍需正視。CMHK的處理方法是盡快向警方反欺騙協調中心（ADDC） 舉報案件，並透過發送短訊、於網站和社交媒體公布消息提醒用戶。此外，中國移動香港客戶服務熱線也會提醒來電者注意近期的詐騙手法。以下是CMHK其中一篇於Facebook上發布的帖文：
「如果大家見到可疑來電，記得要提高警覺，唔好接聽同回撥，時刻保障自己呀！」

作為流動網絡供應商，保護客戶資料對CMHK來說至關重要。CMHK採納不同保安措施來保護客戶的資料和私隱，確保資料不會被挪用作行銷宣傳。CMHK設立獨立資訊科技安全團隊防止電話欺詐，使近年詐騙個案有所下降。除了技術層面

below one thousand cases in 2017, a 4% rebound in the amount of financial loss to HKD229 million has been recorded.

Recently, telephone scammers have used CMHK's channels to conduct telephone deception calls. The scammers often pretend to be staff of CMHK, telling users they have outstanding telephone bills, and providing them with a bank account so that they can wire money in. Fortunately, not many people fell for this scam despite the sheer amount of phone calls made behind this scam. Nonetheless, this scam needs to be addressed. CMHK responded by reporting cases to the police's Anti-Deception Coordination Center (ADDC) as soon as possible, as well as to alert users with mass distribution of text messages, on website, and social media. Additionally, China Mobile's hotline includes a voice recording that warns callers of recent scams.

As a service provider, protecting customer data is of fundamental importance to CMHK. Security measures are implemented to protect customer data and privacy so that such information will not be actively advertised for marketing purposes. An independent IT security team are involved in countering telephone deception, and the trend of successful cases has dropped in recent years. Apart from technical efforts, CMHK actively aids customers to tackle cybercrime by reporting telephone deception cases to the police, educating users, and assisting victims after the fact.

Lee notes that the decline of telephone deception would largely be dependent on the users' awareness of deception tactics. Service providers can do their share of raising awareness via text messages or social media, but the users are the final gatekeeper against cybercrimes.

外，CMHK亦積極協助客戶應對網絡犯罪，包括向警方舉報電話詐騙個案、教育用戶及為受害人提供協助。

李先生指出，要降低電話詐騙個案，主要取決於用戶對欺騙手法的意識。服務供應商當然可以通過短訊或社交媒體提高他們的意識，但用戶才是打擊網絡犯罪的最後防線。