Keeping Cyber Security Ahead of Crime in the 5G Era

3香港提升網絡保安　迎接5G新世代

Hutchison Telecommunications (Hong Kong) Limited
和記電訊(香港)有限公司

In an increasingly digitalised market, cybercrime and telephone deception could be described by the old saying: "As virtue rises one foot, vice rises 10". Ever-more fiendish cyberattacks and phone scams are rightly prompting enterprises and individuals to stay vigilant at all times. 3 Hong Kong is acutely aware of the need to protect itself and customers, as the company transforms from mobile operator to developer of a digital Internet economy via rising levels of sophistication in mobile connectivity, services and content.

在日趨數碼化的市場，網絡攻擊和電話騙案的手法亦越趨複雜和猖狂，堪稱「道高一呎，魔高一丈」，令個人及企業均需時刻保持警覺。隨著3香港逐漸由流動通訊營辦商轉型為數碼互聯網新經濟的發展商，我們所提供的流動連接服務、通訊服務及內容亦更趨精密，故此我們更明白網絡安全對保護公司和客戶的重要性。

3 Hong Kong's digital transformation project involves redesigning IT network infrastructure.
3香港的數碼轉型項目包括重新打造資訊科技網絡基建。

Redesigning IT Infrastructure

3 Hong Kong has established a digital security team dedicated to applying the latest technologies and expertise to making sure cyber security stays at least one step ahead of the criminal underworld. We have embarked on a transformational journey that will help us prepare for 5G, while strengthening internal security and addressing data breaches.

We design IT infrastructure security enhancements and safeguard sensitive data, such as customer and payment information data, according to industrial protocols such as the Payment Card Industry Data Security Standard.

重新設計資訊科技基建

3香港早已成立數碼安全專責小組，採用最新科技和專業知識，應對手法層出不窮的網絡罪案，以確保網絡安全。新開展的數碼轉型項目，既為迎接5G世代，亦同時提升內部保安及防護數據洩漏的風險。

新資訊科技基建均根據行業協定，例如支付卡行業數據安全標準（PCI-DSS）等設計，以加強網絡安全及更有效保障客戶及付款資料等敏感數據。有關數碼轉型項目包括重新打造資訊科技網絡基建，根據不同的用途，分隔網絡部件、系統及平台，

Our digital transformation project involves redesigning IT network infrastructure by partitioning network elements, systems and platforms according to their disparate purposes – all so appropriate levels of security control can be applied. We also deploy a variety of firewalls and anti-DDoS systems.

Expected completion of a four-phrase project in 2020 will also see 3 Hong Kong introducing a "tokenisation" solution. This means sensitive information will be stored in difficult-to-decrypt tokens, thereby reinforcing protection around customer credit card information.

Fending off Cyberattacks and Phone Scams

3 Hong Kong combats cybercrime and telephone deception of all kinds. Common and enduring industry threats revolve around roaming fraud, identity theft, employment traps, phishing email and "one-ring-one-cut" phone scams. This has prompted us to deploy advanced IT systems, along with close monitoring of procedures and processes in order to minimise threats to operations.

Roaming Fraud

Roaming fraud is a mobile-generated, industry-wide problem related to International Revenue Share Fraud. In one category of persistent roaming fraud, users who have handsets stolen overseas end up having to pay massive phone bills, because fraudsters use their handsets or SIMs to make seemingly countless IDD calls. In response, 3 Hong Kong deployed the Fraud Management System to monitor customers' roaming data habits, with a view to suspending service the instant abnormal usage is detected. This highly-effective system has reduced fraud loss that would have otherwise cost customers hundreds of thousands of Hong Kong dollars in each case.

Identity Theft

Fraudsters also steal identities by hijacking mobile numbers or using a victim's SIM card to get free handsets from a mobile operator. After obtaining someone's SIM, these criminals login to the victim's eBanking account to shop online or conduct online transactions. 3 Hong Kong became one of the first service providers to enhance the SIM replacement process in 2018 by sending requests for approval to a customer's email account, or second SIM, using a one-time password to confirm his or her identity beyond doubt.

Employment Trap

This deception involves fraudsters posing as "recruiters" to exploit job seekers desperately looking for quick cash. The targets are asked to subscribe to a monthly plan or handset offer on behalf of a stranger in order to resell popular handsets for profit or obtain personal information with which to apply for a credit card or loan. The job seekers end up being hit by massive telephone bills or other debts. Employment trap deception was widespread in 2011 and remains a threat today. In fact, one victim lost close to HK$1 million back in 2016, according to a news report.

Taking the initiative once again, 3 Hong Kong makes strenuous efforts to keep frontline staff alert to this kind of deception by

3 Hong Kong's digital security team applies the latest technologies and expertise to making sure cyber security stays at least one step ahead of the criminal underworld.
3香港的數碼安全專責小組，採用最新科技和專業知識，應對手法層出不窮的網絡罪案，以確保網絡安全 。

各自採用適合其安全需要的保安措施，並透過不同種類的防火牆及DDoS防禦系統，進一步提升安全度。

數碼轉型項目分四個階段進行，預期於2020年完成，屆時3香港亦已引入「資料代碼化方案」，即以代碼方式儲存敏感資料。由於代碼難以破解，因而能進一步保護客戶信用卡資料的安全。

打擊網絡攻擊及電話騙案

3香港曾處理過各式各樣的網絡罪案和電話騙案，而業內常見的包括漫遊騙案、身份盜竊、求職陷阱、釣魚詐騙電郵和「一響即掛」電話騙案。為打擊這些罪案，我們採用先進的資訊科技系統，並定期密切監察各項程序，減低營運上的威脅。

漫遊騙案

漫遊騙案由流動通訊衍生，與國際利潤攤分騙案（IRSF）息息相關，是業內常見的騙案。其中一種經常發生的漫遊騙案，是用戶於海外被盜取手機，騙徒利用該手機或SIM卡撥打無數的國際長途電話，令用戶須承擔龐大的國際長途電話費。有見及此，3香港特別採用詐騙管理系統，監察客戶的漫遊數據用量，以便在偵察到用量突變時，可瞬即暫停客戶的漫遊服務，減低用戶的損失。此系統高度可靠，曾多次成功偵察到異常用量，每次有效防止客戶損失的金額數以十萬計。

身份盜竊

騙徒亦會騎劫客戶的流動電話號碼或利用他人的SIM卡，盜取別人的身份，騙取流動通訊服務營辦商的免費手機。騙徒獲取他人的SIM卡後，便登入他們的網上銀行賬戶，進行網購或網上交易。為打擊有關騙案，3香港自2018年起，在客戶要求更換SIM卡時，務必先電郵客戶或發短訊至其後備SIM卡，以一

3 Hong Kong pumps considerable effort into raising public awareness around cybercrime and phone deception.
3香港致力喚醒公眾對網絡罪行及電話騙案的關注。

conducting regular briefing and training sessions. Also in place is an effective system of immediate notification on suspicious cases.

Drawing the Public's Attention to Scams

3 Hong Kong works tirelessly to enhance internal security. Considerable effort is also pumped into raising public awareness around cybercrime and phone deception. We publish announcements in newspapers and on websites and social media platforms to alert the public as soon as new forms of deception emerge.

In 2015, an unidentified party made use of Hutchison Telecom Hong Kong's name to set up a bogus company website and fake email address, via which it reached out to the general public. We also became aware of individuals masquerading as 3 Hong Kong staff and calling members of the public under the pretence of promoting mobile renewal offers. In actual fact, they were encouraging their targets to switch to other mobile providers. These individuals provided inaccurate service renewal information and harassed and threatened their targets with foul language.

3 Hong Kong acted immediately by bringing the fraud to light. We alerted the general public and reported the miscreants to the police.

3 Hong Kong takes proactive action to alert customers to new cases of phone deception, and collaborates with police, other industry players and anti-cybercrime associations in the fight against crime.

In 2018, 3 Hong Kong was one of the first operators to alert customers to an industry-wide scam called *Wangiri* or "one ring and cut". This involved fraudsters generating calls from overseas to random mobile phone numbers, then hanging up after one or two rings.

3 Hong Kong received enquiries after customers took unexpected

次性密碼再三核實有關要求；而3香港亦是其中一家最早採用這方式以加強SIM卡更換程序的電訊營辦商。

求職陷阱

有關騙案涉及騙徒偽裝為僱主，誘使求職者「搵快錢」。騙徒要求求職者為陌生人上台或出機，以騙取熱門手機轉售圖利，或盜取求職者的個人資料申請信用卡或貸款，令求職者須承擔龐大的電話費或債項。這類求職陷阱於2011年盛極一時，但至今仍然普遍。根據相關報導，有受害人於2016年損失近百萬港元。

3香港努力不懈打擊這類騙案，不但定期舉行簡報會及培訓，提醒前線員工留意有關騙案；亦設有行之有效的即時通報系統，在有可疑事件發生時立即通知前線員工提高警覺。

喚醒公眾關注網絡罪行

3香港除竭力提升內部網絡保安，亦致力喚醒公眾對網絡罪行及電話騙案的關注。每當遇到新型騙案，我們會迅速透過不同途徑，例如報章、網站及社交媒體平台通知客戶提高警覺。

於2015年，有不明人士以「和記電訊香港」的名義設立虛假的公司網站和電郵，並以此接觸公眾。此外，亦曾有人冒充3香港職員，致電公眾人士假裝宣傳流動電話續約優惠，實為慫恿目標人士轉台。這些人特意提供錯誤的服務續約資訊，並以粗言穢語威嚇目標人士。面對這類「黑白臉」事件，3香港立刻澄清，呼籲市民多加留意，並將事件交由警方處理。

3香港採取主動，知會客戶電騙新招，並與警方、其他業界夥伴及反罪案組織合作，攜手打擊罪案。 2018年，3香港接獲客戶查詢有關收到來歷不明的國際長途電話，例如+678（瓦努阿圖）、+256（烏干達）、+881（銥衛星 Iridium Satellite）、

international calls from obscure country codes such as +678 (Vanuatu), +256(Uganda), +881(Iridium Satellite), +674(Nauru), +675(Papua New Guinea), +676(Tonga) and +685(Samoa). Some returned calls to those numbers and incurred international charges. We were swift to stop the scam spreading by alerting customers via text messages and posting warnings on our website and throughout social media platforms. The media picked up the story and drew the public's attention to the scam.

Stakeholders Must Join Forces to Combat Cybercrime

In another move, 3 Hong Kong supported launch of the Hong Kong Police Force's Anti-Deception Co-ordination Centre by sending SMS to customers in July and December 2017. We also took part in three consecutive years of crisis drills organised by the Hong Kong Computer Emergency Response Team Co-ordination Centre – and remain in touch with international anti-cybercrime associations.

The battle between cybercrime and cyber security shows no sign of abating, as the telecoms industry migrates towards the 5G era and even greater digitalisation. In order to combat cybercrime triumphantly, we – industry players, consumers, police and other stakeholders – must work together, locally and internationally.

+674（那魯 Nauru）、+675（巴布亞新幾內亞 Papua New Guinea）、+676（東加 Tonga）及 +685（薩摩亞 Samoa）等前置地區編號發出之來電，並於一至兩回鈴聲後立即掛線；有客戶回電該等號碼而衍生長途電話費用。

3香港迅即於網站及社交媒體平台刊登啟事及發放短訊，率先提醒客戶留意經常出現於電訊業、名為「Wangiri」或「一響即掛」的詐騙事件，有關貼文引起傳媒廣泛報導，有助阻止騙案蔓延。

持份者聯手打擊網絡罪案

此外，3香港亦支持香港警方成立反詐騙協調中心，分別於2017年7月及12月發短訊，通知客戶有關機構的成立及聯絡方法。我們亦連續三年參與由香港電腦保安事故協調中心舉辦的危機事故演習，並與國際反網絡罪案組織保持聯繫。

隨著電訊業邁向5G世代，數碼化越趨普及，網絡罪案手法亦層出不窮，與網絡保安工作時刻相互逐鹿。要確保成功打擊網絡罪案，相信各持份者，包括業界、消費者和警方同心協力，於本地及國際層面通力合作可謂不二法門。