We Are Becoming More Dependent on the Virtual Realm, but the Virtual Realm Is Simultaneously Becoming More Vulnerable

我們越來越依賴虛擬領域，但它卻漸漸變成危機四伏！

By Hubert Chan & Linus Chan
作者：陳重義、陳賢諾

We are living in a digital age where people use the Internet and the online world for a multitude of purposes. This digital age stems from rapid technological advances in the past few decades. As a result, many facets of life have shifted to the virtual realm. To name a few uses, people can store personal information (e.g. phone numbers and addresses, calendar, books, photos, videos, text messages, Email, Internet history, banking information, passwords), access social networking accounts (e.g. Facebook, Twitter), travel (e.g. Uber, DiDi, Google Maps) and other personal files all on their electronic devices (Mims, 2012). Users can access and "look-up" all sorts of information virtually anytime and anywhere; time and geographical location are no longer constraints. People can communicate with family, friends, associates, and colleagues anytime regardless of where they are. Further, the Internet's anonymity allows users to join online communities such that users can participate in an infinite number of niches such as politics, specified chatrooms, and online forums.

我們生活在一個數碼時代，人人都利用互聯網和網絡世界處理各種需要，這都要歸功於過去數十載科技的迅速發展的成果。因此，我們生活上多方面的需要都轉移到虛擬領域中進行。比如說：儲存個人資料（例如：電話號碼和地址、行事曆、書籍、照片、視頻、短訊、電郵、互聯網瀏覽紀錄、銀行資料和密碼）、使用社交媒體帳戶（例如：臉書、推特）、旅遊（例如：優步、滴滴出行、谷歌地圖）和其他個人檔案都會存儲到他們的電子設備上（Mims，2012）。用戶還可以隨時隨地讀取和「搜尋」各種資料；無論身處何地，人也可以隨時與家人、朋友、伙伴和同事聯繫。此外，互聯網的匿名性允許用戶加入線上社群，讓他們可以參與各種各樣的針尖領域包括政治、專用聊天室和線上論壇。

Despite these vast beneficial changes, one's mere participation in the cyberspace inevitably brings on the risk of cybercrime. As such, we first discuss the practical and psychological dependence of the virtual realm, how the virtual realm gives rise to cybercrime and the need for cybersecurity, and how telephone deception bypasses security measures. Following that, we discuss how leading practitioners in Hong Kong fight against cybercrime, and evaluate how upcoming advances in technology would impact cybercrime. Lastly, we close with the best practices against cybercrime.

儘管這改變帶來巨大好處，但只要輕輕踏進網絡空間便會帶來無可避免的網絡犯罪風險。因此，我們首先要探討對虛擬領域的實用與心理依賴、虛擬領域如何提升網絡犯罪和網絡安全的需求，以及電話詐騙如何避過安全措施。之後我們將探討香港領先的從業者如何打擊網絡犯罪，並探討日新月異的科技如何影響網絡犯罪。最後，我們以打擊網絡犯罪的最佳實踐作總結。

Practical and Psychological Dependence on the Virtual Realm

Since the promulgation of the Internet, we have increasingly included the online world into our lives, to the point we are now highly dependent on it, pragmatically and psychologically.

Pragmatically, storing information digitally eases access and storage space. Consequently, one's data (e.g. personal life and work life files) are often conveniently stored in one's computer, smartphone, in the Cloud, or in the online world. These data include one's search history, online accounts (e.g. airline, banking, social media, and subscriptions), E-books, and digital photo albums etc. But perhaps most striking is how the Internet altered how we communicate. Indeed, the Internet paved the way for Email to be the primary method of communication in the workplace (Burg, 2012), and many people spend up to one-third of their time on computers devoted to email communications (Acton, 2013). Yet, the promulgation of SnapChat and Instagram in the early 2010s influenced the world of social media. Beyond communicating with close ones, many politicians and celebrities use it to communicate with the general public.

However, people who store their personal data digitally put themselves at risk because digital information can be hacked or stolen online, and many people want to acquire sensitive

對虛擬領域的實用與心理依賴

自互聯網開放以來，我們逐漸將網上世界融入生活中。現在，它已成為我們實用與心理上不可或缺的一部份。

實用性方面，以數碼方式存儲資料令讀取和存儲空間更靈活。因此，個人資料（例如：個人生活和工作的文檔）通常可以方便地存儲在個人電腦、智能手機、雲端或線上世界。這些資料包括搜尋紀錄、網上帳戶（例如：航空公司、銀行、社交媒體和訂閱）、電子書和數碼相冊等。但最矚目的是互聯網如何改變我們的溝通方式。實際上，互聯網為電郵成為工作中主要通訊方式而鋪路（Burg，2012），許多人花費自己三分之一的時間處理電郵通訊（Acton，2013）。然而，2010年初SnapChat和Instagram的出現，影響了整個社交媒體界。除了與自己親友交流外，許多的政治家和名人都使用它與公眾進行交流。

但是，人們將個人資料以數碼形式存儲，也是將自己置於風險之中，因為數碼資料可能會被黑客入侵或被盜，而且很多人想獲取敏感的個人資料後可進行操縱（Goldman & Schmalz，2006）。如果個人電腦或手機落入壞人手中，他們會得到事主的個人資料，碰巧是一些敏感文件、圖像或視頻時，事主可能便會被

personal data for manipulation (Goldman & Schmalz, 2006). If one's computer or phone falls into the wrong hands, others will obtain private information about owner, such that people can be blackmailed when sensitive documents, images or videos fall into the wrong hands (FTI Consulting, 2015). Getting involved in the cyberspace poses a risk as there are many ways one's personal data can be obtained. For instance, *cookies* can identify and monitor the activities of web surfers, *viruses* that are inadvertently downloaded can be destructive and wipe out data, *spyware* can track internet use and send that information to third parties, *malware* can damage computer programs, *ransomware* can prevent one from accessing their own files, and *distributed denial of service (DDoS)* renders online services unavailable by flooding it with traffic.

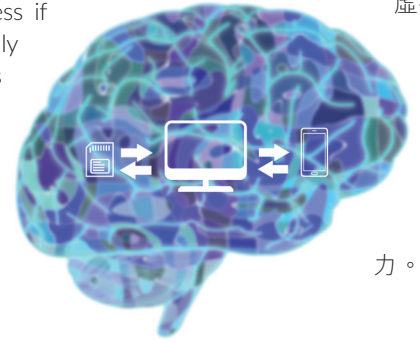
Psychologically, people are dependent on their digital devices. Given that humans cannot encode, store, and retrieve all their knowledge on their own, they offload their memories, schedules, and experiences to external sources. While people used to offload their memories to external sources such as personal journals or friends (Iannone, McCarty, & Kelly, 2016), we now increasingly offload our memories into digital devices (Ward, 2013). This practice of storing one's memories in external devices is known as transactive memory, and people often opt to rely on digital devices instead of other means because the sheer amount of information and storage space outnumbers any other source of transactive memory.

Granted, storing one's information in digital repositories provides immense convenience, but it affects how we remember things. Namely, people tend to report knowing something due to how well they can access it, regardless if the information is stored internally or externally (Mitchell & Johnson, 2000). Psychologists found that the more organized one's digital repositories are, the more confident people report knowing information that can be easily found in digital repositories, even when they do not know the information themselves (Hamilton, McIntyre, & Hertel,

勒索（FTI Consulting，2015）。觸及網絡世界就會存在一定的風險，因為要獲取某人的個人資料實在有太多途徑。例如：*小型文字檔案*（cookie）可以識別和監控網民的活動、*病毒*（viruses）會令你不知不覺間下載具有破壞性及會摧毀的資料、*間諜軟件*（Spyware）可以跟踪互聯網使用情況，並將該資料發送給第三方、*惡意軟件*（Malware）可以破壞電腦程式、*勒索軟件*（Ransomware）可以阻止用戶讀取自己的文檔，而*分散式阻斷服務攻擊*（DDoS）會使網上服務因流量氾濫而無法使用。

心理方面，人往往會依賴於他們的數碼設備。鑑於人類不能自己編碼、存儲和恢復自己所有的知識，所以，只能將記憶、日程安排和經驗轉移到外來資源。雖然人以往常常將記憶轉移到外來資源，例如：記錄個人日誌或與朋友分享（Iannone，McCarty，& Kelly，2016），但現在逐漸地將記憶轉移到數碼設備中（Ward，2013）。這種將個人記憶存儲到外來設備的做法被稱為交互記憶。而由於這些數碼設備具有大量資料和存儲空間，因此人通常選擇依賴它們而不選擇其他方法。

雖然將個人資料存儲到數碼儲存庫為我們帶來無比便利，但它也影響著我們記錄事件的方式。也就是說，無論資料是被存儲於內部還是外部設備，人會傾向根據自己能讀取該事物的情況而作為自己的了解程度（Mitchell & Johnson，2000）。心理學家發現，當人擁有一個有條理的數碼存儲庫時，即使他們本身不了解某方面的知識，他們也會很自信地去表達自己可以從存儲庫中輕鬆找到這些資訊（Hamilton，McIntyre，& Hertel，2016）。換句話說，人更傾向於以他們的虛擬日曆來安排自己的日程。



有時，僅僅是一部智能手機就能耗盡一個人的認知資源，尤其是那些高度依賴手機的人（Ward et al. ，2017）。這種情況的出現，全歸咎於智能手機 - 因它使人可以接通世界，並時刻吸引著他們的注意力。由於注意力是有限資源，那些依賴手機的

2016). In other words, people are more likely to report knowing what their schedule based on how organized their virtual calendar is.

In some cases, the mere presence of one's smartphone can drain one's cognitive resources, especially to those who are highly dependent on one's phone (Ward et al., 2017). This occurs because smartphones – one's gateway to the connected world – constantly take up one's attention. And since attention is a limited resource, people who are reliant on one's smartphone (as a means of transactive memory or communication) often allocate a slice of their attention to inhibit automatic responses to one's phone. Ward et al. (2017) manipulated smartphone salience by having participants either 1) place their devices nearby and in sight, 2) nearby but out of sight, or 3) in a separate room. Participants then completed tasks that measured their cognitive abilities, specifically working memory capacity and fluid intelligence. Results showed that the presence of smartphones was associated with decreased performance on those two tasks, even when participants reported not thinking about the phones.

Beyond personal devices, people are psychologically dependent on the Internet. Although the Internet brings a myriad of benefits, its overuse gave rise to Internet Addiction as a new clinical disorder (Young, 1998), computer vision syndrome (i.e. vision problems linked with using computers; Rosenfield, 2016), and increased reliance on where to find the information instead of actually learning the information (Sparrow, Liu, & Wegner, 2011). Social media use, which is meant to capture and preserve important memories backfires and inhibits how we encode and recall experiences (Tamir et al., 2018). Having the Internet at one's fingertips is no doubt helpful, but people often mistake the Internet's knowledge as their own and lose track of where their knowledge ends and when the Internet begins (Ward, 2013). The Internet inflates how much we think we know; research shows that people often believe the answers they find online are stored in their own mind instead of on the Internet (Fisher, Godu, & Keil, 2015).

人（作為交互記憶或通訊方法）通常很難抑制自己不對手機作出下意識反應。Ward et al.（2017） 進行了以下測試，從中觀察智能手機的操縱性：第一組把手機放在身邊，並且能夠看到；第二組把手機放在身邊，但看不到；第三組把手機放在另一房間中。隨後，參與者完成了幾項認知能力的測試，特別是對工作記憶能力和流體智力的測試。結果顯示，智能手機的存在性對參與者完成兩項測試時的下降表現有關聯，即使參與者反映沒有想著手機。

除了個人設備，人們在心理上都依賴著互聯網。雖然互聯網帶來眾多好處，但濫用互聯網卻引發了新的病症 — 網絡成癮（Young，1998）、電腦視覺綜合症（即因使用電腦而引發的視力問題；Rosenfield，2016），同時也令人傾向找現成的資料，而不是經學習而了解的資料（Sparrow，Liu，& Wegner，2011）。社交媒體的使用，本意是去捕捉和保存重要記憶，如今卻適得其反，壓抑了我們記憶和回憶的技能（Tamir et al.，2018）。無疑觸手可及的互聯網是十分有幫助，但是人往往將互聯網獲得的知識誤認為是自己的知識，更對自己與互聯網的知識來源弄得混淆不清（Ward，2013）。互聯網令人對知識程度自我膨脹；研究顯示人常認為他們在網上找到的答案就是自己的想法，而不是從互聯網上的得到的（Fisher，Godu，& Keil，2015）。

But why are people so drawn towards using the Internet? One reason is that many Internet users are attracted by the Internet's nature of anonymity. On one hand, identity concealment has certain benefits, such as serving as a haven for marginalized groups to communicate with members of the same marginalized group online (McKenna & Bargh, 1998). These marginalized groups are more comfortable expressing concerns or thoughts relevant to their identity online because they can do so anonymously, so the facet of identity they are forced to suppress publicly can emerge authentically online (Jacobton & Donaton, 2009). Consequently, topics that people would like to engage in, but are afraid to do so in a public setting, can be discussed in depth.

However, identity concealment can also be used for malevolent purposes, such as deception and manipulation. Internet users can construct fake identities and detecting deception online is more difficult relative to face to face interaction. For instance, findings have shown that some individuals who claimed to have Munchausen syndrome seek attention and gain sympathy from others (Pulman & Taylor, 2012), indicating how easy it is to create a fake identity that is often difficult for others to detect. Cases like these make people harder to differentiate real identities from fake ones in the cyberworld.

Hancock (2007) classified digital deception into two broad categories. First, identity deception revolves around the creation of a false identity. In the cyberworld, people can lie about their personal information (e.g., age, sex, ethnicity, backstory), and can enter and leave an online context (e.g., a virtual chat room) as frequently as they wish. According to the online disinhibition effect (Suler, 2004), individuals tend to be more comfortable disclosing personal information online than in face-to-face interactions. Past research has shown that people are more likely to tell lies on email and instant messages compared to face to face communication (Naquin, Kutzberg, & Belkin, 2010). Lies are more readily believed online because nonverbal cues present in face-to-face conversations disappear in the online world.

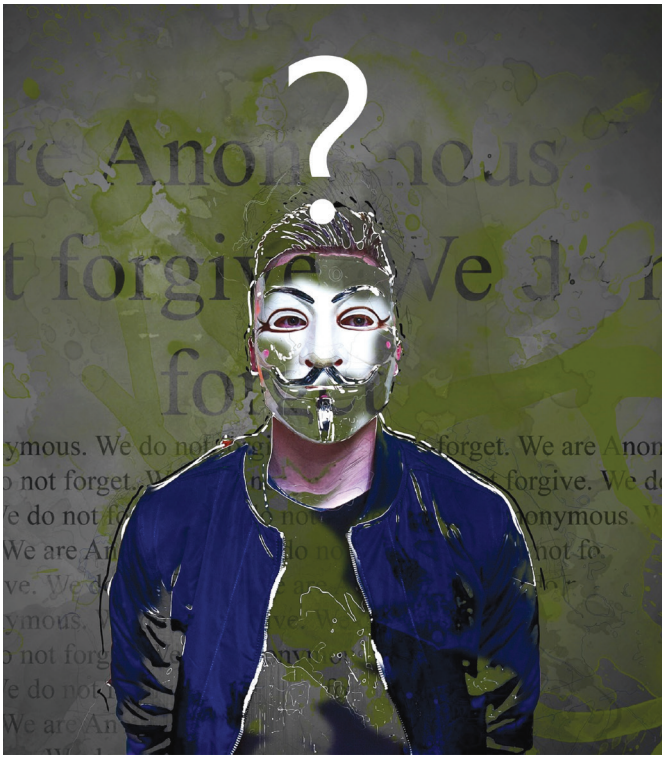
Second, message-based deception relies on fictitious content. If online messages are processed with mental shortcuts instead of thorough thoughts, these viewers may fail to distinguish deceptive messages from authentic ones. This tendency is common because Internet users are bombarded by information overload. As a result, they frequently do not read web messages carefully and instead rely on heuristics, such as making premature judgments of the validity of a messages based on the face validity of the message, credibility of the speaker, or number of arguments (Petty & Cacioppo, 1986; Guo, Trueblood, & Diederich, 2017).

The aforementioned findings indicate that fake identities are easy to create and false messages are easy to circulate, putting Internet users at risk of cybercrimes related to both identity and message-based deception. Because we are increasingly reliant on the virtual realm, we need to the know threats of cybercrime and how it can affect us all.

但為什麼人會如此沉醉於使用互聯網？其中一個原因是互聯網的匿名性質。身份隱瞞具一定的好處，例如：可作為一些非主流群體與相同群體的成員於線上交流的避風港（McKenna＆Bargh，1998），這樣他們便能夠更加自在地在網上匿名發言，表達與他們身份相關的問題或想法，即使他們不能公開身份也可於網上出現（Jacobton＆Donaton，2009）。於是，人便可以毫無顧忌地參與及探討自己喜歡的話題。

然而，身份隱瞞也可被用於一些不良意圖，比如說藉此行使詐騙或進行操縱。網絡用戶可以建立虛假身份，因此要分辨網上騙局便會比面對面交流的困難許多。有調查發現，一些聲稱患有孟喬森綜合症的人在網絡尋求關注，以取得他人的同情（Pulman＆Taylor，2012），這也顯示了建立一個虛假身份是多麼容易，而且通常很難被人發現。因此，這也正正使人難以從網絡世界中的虛假身份分辨真偽。

Hancock（2007）將數碼欺騙分為兩大類。第一類，身份欺騙主要因建立虛假身份而起。在網絡世界中，人可以隨意編造個人資料（例如：年齡、性別、種族、背景），並且可以隨時加入或退出網絡環境（例如：網絡聊天室）。根據網絡去抑制效應（Suler，2004），個人普遍覺得在網上披露個人資料比面對面交流時更加自如。過去有研究顯示，與面對面交流相比之下，人更傾向於在電郵和即時通訊中撒謊（Naquin, Kutzberg，& Belkin, 2010）。而且，於網上撒謊更容易被人相信，因為在網絡世界是看不到面對面交談中出現的非言語表情。



Virtual Realm Gives Rise to Cybercrime

There is abundant personal data stored in different databases that are susceptible to hacking. Cybersecurity does not guarantee 100% protection, so as long as data is stored online, there will be a non-zero chance that sensitive data can be obtained by external parties. For instance, many hospitals store their patient's health records. The automobile sector stores people's driving information. Electronic banking stores people's financial information. These databases, if hacked, would provide cybercriminals with ways to steal, deceive, and manipulate their victims.

Unlike traditional crimes, cybercrime takes on a whole new form that stem from the promulgation of the Internet and advances in technology. Namely, cyberthreats can 1) attack regardless of physical location 2) attack at any time, 3) be anonymous and untraceable in some cases, 4) succeed with only one attempt. As these characteristics heighten the power of cybercrime which in turn call for the need for cybersecurity.

Recently, there were huge data leaks in databases that contains heaps of personal data, including Facebook, MyFitnessPal, Chipotle, Verizon, Whole Food Market, Forever 21, eBay, SnapChat, LinkedIn, and DropBox (Daitch, 2018). Many of these data breaches revolved around payment information and purchase history, but also personal data on social media sites. These data breaches can serve as a cybercriminals' goldmine and calls for the need for cybersecurity.

Fortunately, many extra layers of security are implemented to protect one's privacy in recent years. On individual level, *advanced passwords* decreases the likelihood of others (or A.I. technology) from accurately guessing and entering one's private accounts. *Cloud backups* stores extra copies of data in case hackers erases or shuts down access that data. *Two-factor authentication* protects access to one's accounts by requiring people to provide an additional piece of information after providing one's username and password. This piece of information can be something the user knows (e.g. personal identification number, passwords, answer to security questions), some form of person verification (e.g. voice ID, face ID, fingerprint), or the piece of information is sent to one's electronic devices. Encryption converts data into code and prevents external parties from accessing information sent between parties.

On a broader level, companies secure data (and also their clients/ customers' data) with an array of security measures. Many

第二類，依賴虛構內容的訊息欺騙。人如果只單憑直覺而不經思考去理解網絡資訊的話，根本無法區分資訊的真偽。但這種情況十分普遍，因為網絡用戶經常被大量的資訊轟炸。因此，人往往不會小心地細閱網絡訊息，只憑自己的直觀推斷來下定論，比如根據訊息的表面效度、發言者的可信性或訊息的爭議性（Petty & Cacioppo，1986；Guo，Trueblood，& Diederich，2017）。

上述調查結果顯示，虛假身份容易創建，而虛假消息也易於傳播，與兩者相關的網絡犯罪將使互聯網用戶面臨更大的風險。正因為我們越來越依賴虛擬領域，我們必須要認識到網絡犯罪的威脅以及它會對我們造成何等影響。

虛擬領域引發網絡犯罪

現時有大量的個人資料存儲於不同，且易受黑客攻擊的資料庫裡。網絡安全不能保證有百份百的保護，因此只要資料是存儲於網上，敏感資料便有機會被他人讀取。比如說，許多醫院會存儲其病人的健康紀錄、汽車公司會存儲駕駛者資料和電子銀行會存儲客戶個人財務資料等放在網上資料庫。要是這些資料庫被黑客攻擊了，網絡犯罪分子便有機可乘，去進行竊取、欺騙和操縱受害者。

與傳統罪案不同，網絡犯罪在互聯網的出現及科技進步的推動下，以一種全新形式出現。也就是說網絡威脅具備了以下特點：1) 隨地攻擊；2) 隨時攻擊；3) 匿名且在某些情況下無法追踪；4)一擊即中。這些特點提高了網絡犯罪的威力，相應地網絡安全的需求也就愈發迫切。

最近，臉書、減肥寶、Chipotle墨西哥燒烤快餐店、威瑞森通訊、全食超市、Forever 21、億貝、色拉布、領英和Dropbox（Daitch，2018）等公司都出現了數據庫洩漏資料事件，當中包含大量個人資料。被洩露的資料大多數是與付款和購買紀錄有關，還有就是社交媒體網站上的個人資料。這些被洩露的資料便成為了網絡犯罪分子的金礦，再次體現了網絡安全的迫切需要。

companies recognize cybersecurity as a mission-critical need and implement various security measures as a form of corporate social responsibility. *Threat analysis* keeps a bank of known cyberattacks or viruses, so these attacks can be identified and stopped before they are launched. *Network and service resiliency* reports anomalous data transactions and alerts the appropriate operator or technician for investigation. *Round-the-clock* monitoring refers to teams monitoring for cyberthreats 24/7 with given protocols. Some companies even employ *certified ethical hackers* to conduct threat analysis and weaknesses in their security systems or have their own *security operations center* that actively monitors their customers/clients' data.

Impact of Cyber-hacking

Apart from financial losses, there are long-lasting psychological outcomes when individuals or companies are hacked. The psychological literature indicates that cybercrime victims are affected in many significant ways. First, those who experienced cybercrimes trust the online world less. When people engage in numerous online activities, they are often required to give some personal data (e.g. shipping address for online shopping). However, sensitive information stored in the cyberspace provides opportunities unauthorized third parties such as hackers and phishers. Hence, people will continue to do so if they experience positive outcomes (e.g. online products delivered to one's home), but will likely stop doing it if personal data is hacked (e.g. addresses are unwillingly given away). Once hacked, the user will likely question whether other personal data stored online is safe or vulnerable. The massive data leak from Facebook, for instance, causes privacy concerns for other social media sites (Romano, 2018). Similarly, those who fell for phishing scams before are likely more aware of future phishing scams (Hong, 2012).

Second, those who experience cybercrime tend to experience reduced control and fairness in the online world. This is partly due to the nature of cybercrimes; perpetrators can commit cybercrimes anytime and anywhere, making their identity hard to trace (Naquin, Kurtzberg, & Belkin, 2010). The victim does not know if the hacker is an individual, a team, or part of a larger syndicate. In addition, some cybercrimes are highly sophisticated and victims may not know how to respond or protect their data. Compared to conventional crimes, victims of cybercrime tend to feel more prone to feel helpless (DeTardo-Bora & Bora, 2016), which increases one's perceived loss of control and fairness.

Third, cyberhacking may contaminate the credibility of messages sent online. When people find out that messages - Emails, tweets, fake stories - are posted by bots or by hackers, they may doubt the veracity of other online messages from unfamiliar sources (Vayansky & Kumar, 2018). Bots can be malicious and cause chaos online; they could inflate support for a political candidate (Ratkiewicz et al., 2011), distribute spam of malware on chatrooms (Gianvecchio et al., 2008), or disseminate politically-biased news on social networks (Lokot & Diakopoulos, 2015). Hence, people can confuse messages from unfamiliar sources online because they are not certain whether it come from bots or real people.

幸運地，近年來在保護個人私隱方面實施了多種安全措施。在個人層面，*進階密碼*減低了被人（或人工智能技術）識破和盜用私人賬戶的可能性。*雲備份*可存儲資料備份，以防被黑客刪除或終斷讀取資料。*雙重認證*通過要求用戶在提供用戶名稱和密碼後，額外提供一些資料來保護其帳戶的讀取權，這些資料通常是用戶已知的事項（例如：個人身份証號碼、密碼、保安問題的答案）、其他形式的個人驗證（例如：語音辨識、臉部辨識、指紋），或透過發送驗證碼到用戶的個人電子設備。加密是將資料轉換成代碼，從而防止資料在傳送中被他人讀取。

在更廣泛的層面上，企業會以一系列的安全措施保護資料（以及其客戶/顧客的資料）。許多企業認為網絡安全的需要極其重要，並採取各種安全措施作為他們履行企業社會責任的一種形式。*威脅分析*會保存一系列已知的網絡攻擊或病毒資料，以便識別及阻止其攻擊。*網絡和服務彈性*報告異常資料存取，並通知有關的操作員或技術人員進行調查。*全天候監控*是指以團隊根據協議全天候監控網絡威脅。甚至有些企業會聘請*道德黑客*，對其安全系統進行威脅分析和漏洞測試，或者建立自家的資訊*安全管理中心*主動監控其顧客/客戶的資料。

網絡黑客攻擊的影響

個人或公司遭到黑客攻擊後，除了招致金錢損失外，還會留下長期的心理影響。心理學文獻指出，網絡罪案受害者會受到多方面影響。首先，網絡罪案受害者會對網絡世界的信任降低。當人使用網絡時，經常需要提供某些個人資料（例如：網購的送貨地址）。但是，存儲在網絡空間中的敏感資料，正正為未經授權的第三方比如黑客和網絡釣魚者提供竊取機會。要是客戶體驗到滿意的網上服務（例如：網購的物品安全送達），他們會繼續使用；要是客戶的個人資料遭到黑客攻擊（例如：地址洩露），他們很可能從此不會再使用這服務。一旦被黑客攻擊，用戶會對自己儲存在網上的資料是否安全而存疑。例如：洩露了大量資料的臉書，就引起了其他社交媒體網站對私隱問題的關注（Romano，2018）。同樣，曾誤墮網路釣魚騙案的人，會對往後的網路釣魚詐騙更為警惕（Hong，2012）。

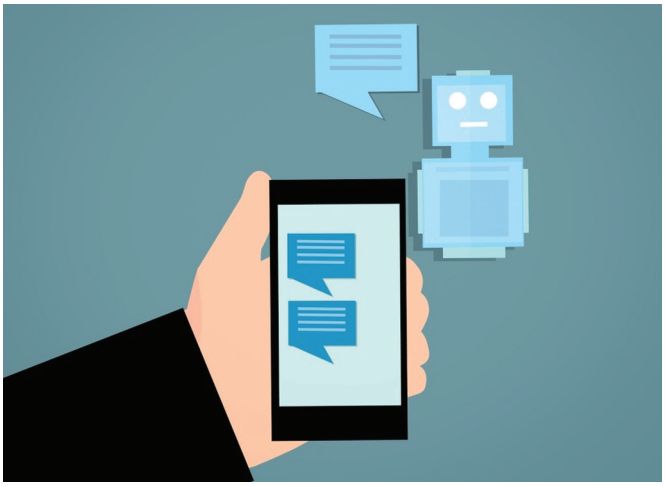
其次，網絡罪案受害者會體會到網絡世界的疏於監管和公平待遇。這可歸因於網絡罪案的特性 - 犯罪者可以隨時隨地進行網絡犯罪，並使其身份難以追查（Naquin，Kurtzberg，&Belkin，2010）。受害者不會知道作案的是個體、團隊，或者說是某個大集團的一部份。此外，有些網絡罪案非常複雜，使受害者不知道如何應對或如何保護其個人資料。網絡罪案受害者往往比傳統罪案的受害者更感到無助（DeTardo-Bora&Bora，2016），最終導致他們對網絡世界缺乏監管和公平待遇的感覺變得更加強烈。

第三，網絡黑客攻擊可能損毀網絡訊息的可信性。當人發現自己收到的電郵、推文或虛假報導之類的訊息是從機器人或黑客

The psychological effects of decreased trust online, reduced control and fairness, along with contaminated message can all affect the user simultaneously in some contexts. For example, online dating scams occur when cybercriminals initiating a fictitious romantic relationship with the intention of defrauding their victims of huge sums of money (Whitty & Buchanan, 2016). In these scenarios, scammers use fictitious profiles on sites with fake photographs and fake backstories. The scammer utilizes this fictitious identity to get closer with their victims and eventually ask them for money. The process of gaining the victim's trust includes declaring one's love and the intention of starting an exclusive relationship with the victim, followed by frequent and intense communications. The scammer will then ask for gifts that increase in value over time. When the victim finds out the online romance is a scam, some reported that the emotional loss was more damaging than financial loss, some had issues coping, and some had a negative view of online relationships.

Another common context of cybercrime victimization are phishing scams. These scams are a type of social engineering in which a "phisher" tries to retrieve confidential information by feigning to be a trustworthy source (Davison & Silence, 2010). Phishing emails are rather easy for perpetrators to send in large volumes (Kaspersky, 2013). In some cases, the Emails resemble familiar sites such as Google Docs (cson, 2017), or the Email

follows conventions in a given genre to look more believable (Chiluwa, 2009). If one falls for phishing Emails and compromise their personal information and identity, Email scams can spread exponentially by exploiting information such as email account holders'. Alternatively, perpetrators can go through a victim's series of email to thoroughly understand his or her work, family, and personal details. Phishing scams that are tailored to specific persons – which include personalized messages – are known as *spearphishing*.



發出的時候，他們可能會懷疑其他來自陌生網站的訊息的真實性（Vayansky＆Kumar，2018）。機器人發出的訊息可以是惡意，並使網絡世界動盪不安。比如說，它們可能會誇大對政治候選人的支持率（Ratkiewicz et al.，2011）、可能於聊天室發佈帶惡意軟件的垃圾郵件（Gianvecchioetal.，2008），還可能在社交網絡上散播有政治偏見的新聞（Lokot＆Diakopoulos，2015）。因此，人便會混淆來自陌生網站的訊息，因為他們不能判斷訊息的真偽。

除了對網絡信心下降、疏於監管和公平待遇的心理影響外，這些被損毀的訊息也同時在其他方面影響著用戶。例如：網上情緣騙案出現就是當網絡犯罪分子為受害者營造出一種虛假的戀愛氣氛，意圖欺騙其巨額金錢（Whitty＆Buchanan，2016）。在這些情況下，騙子借助一些假照片和假背景於網站上虛構個人檔案，然後利用虛構的身份來與受害者建立親密的關係，最終向他們索取金錢。為增加受害者的信任，騙徒會向受害者表達愛意，以及表明想跟受害者發展戀愛關係的意向，然後就是以頻繁和緊密的通訊纏繞著受害者。久而久之，騙徒便開始要求一些越來越貴的禮物。但當受害者發現自己墜入網上情緣騙局時，有些人會覺得感情損失比經濟損失更重、有些人不知如何應對，還有些人從此對網絡戀情抱著負面態度。

另一種常見的網絡罪案是網絡釣魚詐騙。這種詐騙是一種社交工程，「網絡釣魚者」偽裝成有信譽的機構並試圖讀取機密資料（Davison＆Silence，2010）。騙徒可以輕鬆地發送大量釣魚郵件（卡巴斯基，2013）。有時，這些電子郵件會與一些公眾熟悉的網站相似，例如：谷歌文檔（cson，2017）。有時，這些電子郵件會使用慣常格式，從而看起來更加可信（Chiluwa，2009）。如果有人落入了釣魚郵件的圈套，並且披露了個人資料以及身份訊息，詐騙電郵就能利用獲取的資料，如郵件賬戶持有者的資料，來進行爆炸式傳播。或者，騙徒可以透過受害者的電子郵件徹底掌握受害者的工作、家庭及個人各方面細節。此外，網絡釣魚詐騙還有一種魚叉式*釣魚詐騙*，這種詐騙手段是針對特定人仕以個人化資料而定制的騙局。

Unfortunately, individuals who use computers more may be less cautious of cybercrime threats in the long run due to habituation. For instance, heavy users who spend eight hours a day on a computer are more likely to habituate to the routine checking and replying to emails than casual users who only spend an hour a day. Research suggest that email habit strength, or the tendency to routinely open one's email account without active deliberations, predicted greater susceptibility to phishing scams (Viswanath, 2015). This study also revealed that users who habitually used Facebook to maintain and expand their social networks seldom scanned for deception on this social network site (Viswanath, 2015). Connecting to a large social network increases the difficulty of distinguishing a friend from a stranger, where frequent use of Facebook induces individuals to neglect subtleties that might unveil deception. Fortunately, some research has shown that changes in online behavior when they are aware of risk susceptibility to phishing (Davinson & Silence, 2010).

To defend oneself against cybercrime, one should be concerned about privacy practices online and adopt behaviors that promote privacy. Jensen et al. (2005) had participants report their privacy attitudes then engage in a simulated e-commerce scenario that utilized twelve independent variables that were either present or absent. These are: Item price, secure-socket-layer, third-party cookies, provided an Email address, provided a telephone number, provided the company's postal-code, privacy seal (TRUSTe), credit card symbols (e.g. Visa, Mastercard), and policies surrounding data privacy. Results found that people consider privacy policies more than other factors, and those who are shown more cues (i.e. were shown more of the variables listed above) were more confident in the e-commerce's data security. This suggests that we should look into data security cues to determine the legitimacy of an online site before engaging in any sort of behavior.

These all illustrate how our online behavior can contribute or buffer against cybercrime victimization. Indeed, we are vulnerable in the cyber realm and what happens there affects our psychological well-being on multiple dimensions.

可惜的是，人愈習以為常地長期使用電腦，他們對於網絡犯罪愈不太謹慎。例如：平均每天花八小時在電腦上的高度使用者比每天只花費一小時的一般使用者更易習慣做例行檢查和回覆電郵。研究顯示，習慣使用電郵的人，或是慣於隨意打開電子郵箱的人，預料是最容易受到網絡釣魚詐騙影響的（Viswanath，2015）。該研究還顯示，習慣使用臉書來聯繫朋友和擴展其社交網絡的用戶，很少會提防社交媒體上的詐騙（Viswanath，2015）。大型社交網絡會使用戶難以從陌生人中區分朋友，再者經常使用臉書會導致用戶忽視了捅破騙局的微妙關聯。幸好，有些研究指出，當人意識到網絡釣魚詐騙的風險時，他們會相應地改變自己的網上態度（Davinson & Silence，2010）。

為了打擊網絡犯罪，我們應該關注網絡私隱的實施和採納推廣私隱的態度。 Jensen et al. （2005） 讓參予者申報自己的隱私態度後，安排他們參與一個模擬的電子商貿體驗，並利用十二個可加減的獨立變數，這些變數分別是：商品價格、安全通訊端層、第三方Cookie、預設的電郵地址、預設的電話號碼、預設的公司郵政編碼、隱私標章 （TRUSTe）、信用卡標誌（如：Visa、萬事達卡），以及有關資料私隱的政策。結果顯示，相比其他因素而言，人會比較關注私隱政策；而那些提出更多因素（即上面列出的更多變量）的人對電子商貿的資料安全也更有信心。也就是說，我們應該多了解資料安全有關的資訊，從而去判斷網站的合法性，才進行各種交易活動。

以上說明了我們的網絡行為，如何為打擊和減少網絡犯罪作出貢獻。確實，我們在網絡世界中是易受攻擊，一些風吹草動也會影響著我們多方面的心理健康。

電話詐騙破解了安全措施

儘管已經有大量安全措施設計來保護個人資料和防止網絡黑客攻擊，但仍有辦法可以繞過先進的安全措施從而獲取敏感訊息。網絡安全的進步可以非常有效，但它不能保護最脆弱的一環：人類（米特尼克，2017年）。

「攻擊」人類訊息的人被稱為社交工程師。社交工程師使用各種手段，多數包括操縱、詐騙或直接勒索，去獲取某人的個人資料。由於網絡安全將資料以安全檔案來保護，因此社交工程以電話詐騙方式顯得更為有效。據香港警方統計數字顯示，電話騙案於2016年及2017年所造成的損失金額分別是2.21億港元及2.29億港元。

社交工程師或電話騙徒使用五花八門的手段，套取受害者的個人資料或騙取金錢。為達到目的，他們通常會表現得十分友善並給人一種*可信任*的感覺。最終與受害者建立融洽關係，從而達到自己的目的。也有可能，騙徒會以不友善的語氣去威脅受害者。無論是善或惡，騙徒也可以假冒官員身份去博取受害者的信任。香

Telephone Deception Bypasses Security Measures

Despite heavy security measures designed to protect personal data and prevent cyberhacking, there are still ways to circumvent advanced security and obtain sensitive information. Advances in cybersecurity can be highly potent, but those do not stop the weakest link: the human (Mitnick, 2017).

People who "hack" humans are known as social engineers. Social engineers uses a variety of tactics – most of which include manipulation, deception or straight-up blackmail - to gain access to a person's personal information. Because cybersecurity protects data contained within secure files, social engineering is quite effective via telephone deception. Statistics from the Hong Kong Police show a loss of 221 million HKD in 2016 and 229 million HKD in 2017 due to telephone deception.

Social engineers or telephone scammers use numerous ploys to deceive victims into divulging their information or to get payment. They often do so by exuding *likability* and *credibility*. Scammers aim to build rapport to elicit victims into giving them what they want. Alternatively, scammers may opt to threaten their target with a hostile tone. Friendly or hostile, scammers also assume an authoritative identity in order to gain the trust of the victim. The most common tactics as reported by the Hong Kong Police are: 1) Detained son/fake kidnapping, 2) Guess who I am, 3) pretending official. Telephone scammers may tell their targets that they kidnapped one of their family members and demand money for their release. The swindlers manipulate the elderly by making them worry about their families' safety. Scammers may also pretend to be an official (e.g. immigration official) to demand payment or elicit personal information for "verification". Lastly, scammers call their victims, ask "guess who I am" and wait for the victim to ask some questions (e.g. "are you my former colleague?") to figure out who the caller is. The caller would claim to be one of the names the victim asks and assumes that identity to ask for favors or excuses to scam for money.

Hong Kong Police's Statistics on Telephone Deception

According to statistics provided by the Hong Kong police, cases of telephone deception has decreased steadily (1623 reported cases in 2007, 991 reported cases in 2017), but the money lost has increased. Most cases fall around counterfeit officials, followed by imaginary kidnapping, and "guess who I am".

Over the years, counterfeit officials remained as the most popular modus operandi for telephone deception. In many cases, the fraudsters use modified call identification to impersonate local phone numbers to call the victim and gain his/her trust. Many telephone scammers pose as staff members of the government, logistics companies or other public and private organizations. Once the victim responds to the fraudulent call, the call will be redirected to a fraudster who impersonates a Mainland official.

港警方指出，最常見電話騙案手法是：1)虛構綁架、2)猜猜我是誰、3)假冒官員。電話騙徒會訛稱受害者的家屬被綁架並索取贖金。騙子也會讓長者擔心其家人的安全從而達到操控的目的。騙徒也可能偽裝成官員（例如：入境處官員）去要求付款或誘出個人資料來進行「認證」。還有，騙徒會致電給受害者，以「猜猜我是誰」來等待受害者（例如：你是我以前的同事嗎？）查問其身份，然後訛稱自己就是受害者口中的一個人，順勢祈求幫助或藉口騙錢。

Loss Amount 損失金額	2017 Jan to Jun 1至6月 (Million 百萬元)	2018 Jan to Jun 1至6月 (Million 百萬元)	Comparison 比較	
			Loss Amount 損失金額 (Million 百萬元)	%
Detained Son 虛構綁架	2.16	0.94	-1.22	-56.5
Guess Who I Am 猜猜我是誰	4.42	4.94	+0.52	+11.8
Pretend Official 假冒官員	109.64	4.67	-104.97	-95.7
Other Tactics 其他種類	31.03	0	-31.03	-100
Total 總數	147.25	10.55	-136.7	-92.8

香港警方電話騙案統計數字

根據香港警方提供的統計數據，電話騙案數目穩步下降（2007年錄得1623宗；2017年錄得991宗），但涉案之損失金額卻有所增加。大多數案件都是「假冒官員」、其次就是「虛構綁架」和「猜猜我是誰」這兩種情況。

多年來，「假冒官員」仍然是最常見的電話騙案手法。通常，騙徒會修改來電身份以圖冒充本地號碼從而獲取受害者的信任。甚至有些騙徒會冒充政府官員、物流公司或其他公私營機構的員工。一旦受害者回應騙徒，電話就會轉駁到另一位冒充內地官員的搭檔。

Lessons from Exceptional Leaders

The literature on cybercrime and telephone deception all point to the need for cybersecurity and education on combating cybercrime. As such, CAHK conducted a series of interviews with leading practitioners to better understand how cybercrime and telephone deception is addressed in Hong Kong from multiple perspectives. These parties include vendors, phone operators, Hong Kong police, lawyers, and others. We highlight some key points from the interviews below in alphabetical order of the leader's surname listed below; full interview reports are included in this Guide.

傑出領袖的經驗之談

關於網絡犯罪和電話詐騙的文獻中都指出，網絡安全與打擊網絡犯罪的教育工作的必要性。因此，香港通訊業聯會採訪了一些知名的業內人士，從而更清晰了解香港是如何從多角度解決網絡犯罪和電話詐騙問題。其中包括供應商、電訊營辦商、香港警務處和律師等。我們下面列舉一些採訪中的要點（依英文姓氏字母排列）；全篇專訪內容編排於封面故事之後。

Group Managing Director of HKT* – Mr. Alex Arena

香港電訊集團董事總經理 — 艾維朗先生

* Ms. Susanna Hui has taken up the position of Group Managing Director of HKT following Mr. Alex Arena's retirement on August 31, 2018.

* 艾維朗先生已於2018年8月31日退休，香港電訊集團董事總經理由許漢卿女士接任。

HKT is currently a service provider in Hong Kong with the biggest number of fixed networks and broadbands. HKT is committed to upholding their customer's privacy and does not monitor calls. According to Arena, in order for telecommunication to take place, at least two parties must be present: the sender and the receiver. Hong Kong Telecommunications (HKT) Ltd. provides highly safe and secure communication channel between A to B, and as of now, HKT has faced no serious intrusion into their networks. But even so, this does not mean there are not risks present in A and in B.

The fraudsters' methods evolve alongside communication methods. Scams used to be conveyed through physical means such as leaving leaflets in mailboxes, but now scammers can target people's data in the online world via telecommunications regardless of where the scammer is geographically. HKT's Security Operations Center's analysts help customers detect, respond, and run forensics for their infrastructure. HKT's huge customer base creates a valuable pool of threat intelligence, and analysts have gone through a series of globally recognized trainings in overseas, so that the most advanced cyber security detection technique could be applied to customer's environment.

香港電訊是目前香港擁有最多的固網和寬頻服務的服務供應商。香港電訊致力維護客戶私隱，決不監察電話。據艾維朗先生說，電訊流程最少涉及兩方面：發送者和接收者。香港電訊有限公司為A和B之間提供高度安全和穩妥的通訊途徑，直至目前為止，香港電訊的網絡並無遇到嚴重的入侵事故，但這並不表示A和B的用戶網絡沒有風險存在。

隨著通訊方式日新月異，騙徒的手法亦逐步演變。過往騙徒會親身發放詐騙訊息，例如把單張放進別人的信箱，現在無論騙徒身處何方，都可以通過互聯網入侵他人在網絡世界的資料。香港電訊的資訊安全管理中心資訊科技保安分析人員協助客戶檢測、應對，並為客戶基礎設施進行鑑證。香港電訊憑著龐大的客戶基礎，創造了寶貴的網絡威脅智能訊息庫，同時，分析人員都已通過一系列獲全球認可的培訓，所以最先進的網絡安全檢測和分析技術能夠應用於香港電訊的客戶環境中。

Hong Kong Police Force – Superintendent – Mr. George Chan Senior inspectors – Mr. Andy Chan & Ms. Yonny Yeung 香港警察 — 警司 — 陳天柱先生 高級督察 — 陳國偉先生及 楊蓉小姐	To fight against telephone deception, the Hong Kong Police Force established the Anti-Deception Coordination Centre (ADCC) that is dedicated to all types of deceptions and frauds, including telephone deception. To encourage telephone deception victims to report their case, ADCC provides a one-stop hotline service where victims can call (+852) 18222 for consultation on suspected deceptions without divulging their personal details. ADCC actively supports victims of deception: from advising the potential victim if the phone call is a scam, collating useful information provided by the victim, to engaging the community in anti-scam publicity and partnerships. According to the superintendent and senior inspectors, telephone scammers try to fit in the "right script" according to the victim's profile upon making the cold calls. For instance, to those non local citizens with conditional stay in Hong Kong (e.g. foreign students or workers who temporarily stay in Hong Kong), scammers pretend to be immigration officers or official authorities of their home countries and demand money to solve certain visa issues that, if not met, might result in deportation. To the elderly, scammers may tell them that their children are kidnapped to extort ransom money. To the youth, scammers may impersonate an authority figure to demand personal details. In addition, the ADCC also takes action to intercept ongoing deceptions. If the situation is warranted, police officers will be dispatched onto the scene to offer immediate assistance. 為打擊電話騙案，香港警務處成立了反詐騙協調中心(ADCC)，專責打擊各類型騙案包括電話騙案。為鼓勵騙案受害者及早尋求警方協助，ADCC提供一站式諮詢熱線服務(+852)18222，受害者可就懷疑騙案進行諮詢，而毋須透露其個人資料。ADCC積極為受害者提供支援：如對受害者提供如何應對電話騙案的意見，收集受害者提供的案件資料，還推動社會各界參與反詐騙宣傳及合作。 據警司及高級督察指出，騙徒會根據目標人士的背景而準備好預設對白。例如：對那些非本地居民（如：暫獲留港的外地留學生或工人），騙徒會假冒入境處或當地執法機關官員，要求他們付款來解決某些簽證問題，否則會被驅逐出境；長者方面，騙徒會以虛構綁架的藉口，向他們索取贖金；青少年方面，騙徒會冒充執法機關來獲取他們的個人資料。此外，ADCC亦會採取行動，阻止正在進行的詐騙活動。在必要時，中心會派員到現場向市民提供即時協助。
CEO of CITIC Telecom International CPC Limited – Mr. Stephen Ho 中信國際電訊（信息技術）有限公司 行政總裁 — 何偉中先生	CITIC Telecom CPC service serves as a one-stop-shop that provides enterprises with a full spectrum of ICT solutions across many countries. CITIC employs certified ethical hackers to evaluate CITIC are security and assesses potential areas of improvement. Ho notes that the need for cybersecurity increased over the years because of awareness of high-profile hacks and top-down initiatives. The banking and finance industries, for instance, implemented mandatory protection policies, which in turn drove up the awareness of the importance of security. Advances in technology such as 5G will continue to create opportunities for cybercrime. When devices are linked together, they are prone to security breaches. For instance, Internet of Things rely on sensors (e.g. temperature, light, CCTV cameras) that send out signals when a predetermined stimulus is detected, such as if a room falls below a certain temperature, or turning on the lights if there is movement. These sensors can be prone to security breaches. The rise in telephone deception cases, as well as hijacking texting services from others, led to the loss of millions of dollars. Telephone scammers can have their caller IDs appear as a certain number and can leave no trail behind. Once a victim falls prey, there is no way to reverse the process. 中信國際電訊CPC為多個國家企業提供一站式全方位ICT解決方案。中信聘請「道德黑客」去評估中信基礎設施的安全性及需要改善的地方。何先生指出，由於公眾對網絡威脅的關注和認知提高了，所以，網絡安全的需求也越來越多。例如：銀行及金融服務業，實施了不同的強制性監管政策，同時也提高了個人對安全重要性的認識。 科技的進步為我們帶來5G技術，但也繼續為網絡犯罪創造機會。正因各種設備互聯互通，所以便容易出現安全漏洞。正如物聯網依賴於各種感應器設備（如：温度、燈光或閉路電視攝影機），這些設備會因應房間低於某個溫度抑或檢測到某物體移動，便會發出提示訊號。正因為被廣泛應用，這些設備都容易出現安全漏洞。 電話騙案與劫持短訊案同樣地有所增加，而涉及之損失金額已達數百萬美元。電話騙徒可以將其來電顯示設置為特定號碼，並不會留下任何蛛絲馬跡，受害者一旦落套將無法翻身。

Partner of Mayer Brown and Legal Advisor to CAHK – Ms. Gabriela Kennedy 孖士打律師行合夥人兼香港通訊業聯會法律顧問 — 甘乃迪女士	Many Hong Kong citizens adopt the latest technology (e.g., newest smartphone models), but they tend to use only a fraction of what their device can do. Compared to citizens in Mainland China who integrate e-commerce, WeChat, and online shopping into their lifestyle, the average HK citizens do not utilize the full potential of technology. This may be why cybercrime methods, which are very creative, are quite effective. Social engineers can capitalize on their targets' social media to learn the patterns, lifestyle, and habits of their targeted persons. Examples include fake Job listings, identity theft, smartphone apps, public Wi-Fi, public surveillance, malicious USB drives. When social engineers use personal information for manipulation from overseas, it becomes difficult to punish those responsible and to obtain evidence. Nevertheless, it is still possible to trace back where data is sent, but it takes time and money. Yet, because cyberattacks are of fundamental concern, spending money on IT and security is needed. The issue arises when small-to-mid enterprises with limited resources face the dilemma of deciding how much to invest in cybersecurity. Kennedy supports the IT industry in educating the general public. 許多香港市民採用最新的科技（例如：最新的智能手機型號），但他們往往只使用設備功能的一小部分。與將電子商務、微信和網上購物融入生活方式的中國內地市民相比，香港市民並沒有充分利用科技的全部潛能。因此，便造就網絡犯罪的手段甚具創造性，且能在香港猖獗盛行的原因。社交工程師可以利用目標人群的社交媒體來了解目標人群的模式、生活方式和習慣。例如：虛假招聘啟事、身份盜竊、智能手機應用程式、公共Wi-Fi網絡、公眾監察、惡意USB驅動器等。當海外社交工程師利用個人資料進行欺詐時，在香港却很難懲罰需要負上責任的人，也很難獲得起訴的必要證據。儘管如此，發送資料的地方仍有機會追溯得到，但却需要時間和金錢。 然而，在資訊科技和網絡安全上投放金錢是確保個人在線安全的關鍵。當資源有限的中小企要決定在網絡安全上投資多少金錢而面臨兩難境地時，問題就出現了。甘乃迪女士支持資訊科技界為公眾提供更多的網絡教育。
HGC Global Communications Limited – Mr. Andrew Kwok, CEO Ms. Jacqueline Teo, Chief Digital Officer Mr. Eric Chan, Director of Network and Products 環球全域電訊有限公司 行政總裁 — 郭詠邦先生 首席數碼官 — Ms. Jacqueline Teo 網絡及產品總監 — 陳思源先生	HGC is a fixed-line operator and ICT solutions provider that serves corporations, small to mid-sized enterprises, families, and carriers across many countries around the world. HGC has a 24 x 7 network operating center that oversees all of Hong Kong's networks. In addition, HGC has a security operating center (SOC) responsible for security activities such as data loss prevention. Globally, there are many cases of Distributed Denial of Service (DDos) attacks that utilizes machines and IOT devices to generate "dirty traffic" that shuts down a targeted network. HGC's anti-DDos service helps clients anticipate abnormal network activities before the network is jammed. The anti-DDOS service diverts the traffic to SOC's computers to filter out the dirty traffic and restore normal activities as if no DDoS has occurred. HGC splits telephone deception into two categories: fixed-line and mobile. Since out going fixed-line calls from HGC does not allow modified call-line-identification (CLI), cybercriminals won't be able to modify CLI to trick victims into believing calls come from someone familiar (e.g. one's boss, spouse, daughter). HGC tries to locate the origin of suspicious calls by collaborating with upstream operators and works with mobile operators so outgoing calls that use HGC's network will have a "+" sign added. Denoting that calls are from overseas help warn users of potential suspicious activity. 環球全域電訊有限公司（以下簡稱HGC）是電訊固網服務和資訊科技（ICT）方案營辦商，服務對象包括跨國企業、中小企業、住宅用戶和世界各地其他網絡商。HGC擁有24 x 7 全天候網絡監控中心實時監測全港網絡。同時，HGC的資訊安全管理中心（SOC）負責解決安全相關的問題，包括防止資料洩漏。在全球範圍內，分散式阻斷服務攻擊（DDoS）的案例眾多，通過利用機器和物聯網設備發出大量「垃圾郵件」務求使目標網絡癱瘓。HGC的DDoS防禦服務可以幫助客戶檢測網絡的異常流量，防止網絡癱瘓。DDoS防禦服務通過網絡安全運作中心為客戶攔截攻擊性流量，確保客戶業務正常運作。 HGC將電話騙案分成兩大類型：固網和流動網絡。由於通過HGC的固網撥出的電話不能修改其主叫線路識別（CLI），因此網絡犯罪份子不能通過修改主叫線路識別去誆騙受害人，讓受害人相信電話是來自熟悉的人（如：老闆、配偶或子女）。此外，通過與上游營辦商和流動網絡營辦商合作，HGC能夠通過定位並以「+」標識可疑來電的撥出地區，表明該電話是來自海外，提醒用戶以防受騙。

Chairman & CEO of WiseSpot Company Limited – Mr. Franky Lai 斯博有限公司 主席及行政總裁 — 賴永雄先生	WiseSpot is a provider in telecommunications services that works with significant telecom operators and enterprises in Hong Kong, mainland China, and various other countries. Lai notes that cybercrime is already very common, there is no foreseeable decline in cybercrime in the near future, and we are dealing with risks of data breaches every day. This trend occurs partly engaging in cybercrime is a lucrative endeavor and is associated with high chances of success and low chances of getting caught. Hence, WiseSpot treats cybersecurity as a hygiene factor; hygiene factors are aspects of a business that is essential for survival, and this includes cybersecurity because services cannot sell without security. Lai notes that both carriers and users need to fight against cybercrime. Though carriers tend to focus purely on services (i.e., phone plans) and not consider security, security must now be regarded as a vital hygiene factor because digital transformation has made cybercrime easier. Carriers should perform active vulnerability monitoring to detect online activities because cybercriminals often erase their digital footprints to eliminate chances of getting caught. Users, on the other hand, have to be diligent in securing their data and not blindly open any files, links, or documents that are sent to them. Users need to recognize the risk of opening a malicious link and take precautionary measures to ensure what they click on is safe. 斯博是一家電訊服務供應商，與香港、內地和其他國家重要的電信業運營商和企業合作。賴先生指出，網絡犯罪已經非常普遍，而且至少在可預見的未來，沒有任何下降的跡象，我們每天都面對資料被洩露的風險。這種令人擔憂的趨勢很可能是由於網絡犯罪是一種有利可圖的行為，成功的機率很高，被抓住的機率很低。因此，斯博把網絡安全視為一種保健因素，保健因素是企業生存的必需品，其中包括網絡安全，因為沒有網絡安全的服務是沒有客戶願意購買的。 賴先生還指出，電訊商和用戶需要賂心協力打擊網絡犯罪。儘管，電訊商只純粹專注服務方面（即電話月費計劃）而不考慮安全性問題。但現在數碼化轉型使網絡犯罪有機可乘，電訊商不能再坐視不理保健因素的安全性問題。網絡犯罪分子經常刪除他們的瀏覽足跡以消除被抓住的可能性，所以電訊商應該主動進行漏洞監控以檢測異常活動。另一方面，用戶必須勤於保護自己的資料，不能盲目地打開任何收到的文檔、鏈接或文件。用戶需要認識到點擊惡意鏈接的風險，並採取預防措施以確保他們點擊的內容是安全的。
CEO of BlueSky – Mr. Bernard Lee 藍天專業服務 有限公司 行政總裁 — 李本立先生	BlueSky is currently developing a software platform for MSSP (Managed Security Service Provider). Similar to Uber or DiDi where customers can hire a ride without purchasing the car, clients can hire security service providers on-demand without purchasing the whole security package. Because of this, they are in a sharing economy, and this platform shall let them, and other qualified and highly trained independent cyber security service providers manage lots of small to medium businesses at a lower cost because of efficiency. Lee notes that cybersecurity is important, but the key factors contributing to the global shortage in cybersecurity staff are (a) shortage of qualified personnel; (b) insufficient understanding among leaders; (c) lack of budget in business; (d) difficult to retain qualified personnel; and (e) lack of career path in the industry. Lee stresses that security measures today are highly sophisticated such that the strongest computers cannot crack encryption mathematically. Movies that feature hacking into advanced security systems within a short timespan are a myth. Hacking merely though a computer is impossible without the aid of social engineering (i.e. manipulating and deceiving people to obtain information). Hence, Lee advises enterprises to not only adopt cybersecurity services, but also defense against social engineering tactics. The biggest vulnerability is the human. BlueSky目前正為託管安全服務供應商（MSSP）開發一個軟件平台。與優步或滴滴類似，客戶無需購買汽車下租用車輛，客戶可以按需要而租用安全服務供應商，而無需購置整個服務。正因為如此，客戶處於共享經濟中，這個平台讓客戶，以及其他合資格、受過專業訓練的獨立網絡安全服務供應商，可以以高效率但較低的成本管理大量中小企業務。李先生指出網絡安全十分重要，但造成全球短缺網絡安全人員的關鍵因素是（a）缺乏合資格人員；（b）領導人之間的理解不足；（c）缺乏商業預算；（d）難以挽留合資格人員；（e）缺乏職業發展前景。 李先生強調今天的安全措施非常複雜，即使超級電腦都無法用數學方法破解良好的加密技術。電影中在短時間內入侵先進的安全系統絕對是一個神話。如果沒有社交工程的輔助（例如：操縱和欺騙我們讀取訊息），僅僅通過一台安全的電腦來進行黑客攻擊是不可能的。因此，李先生建議企業不僅要採用網絡安全服務，還要防範社交工程手法。因為最大的漏洞就是人類。

Director & CEO of China Mobile Hong Kong Company Limited – Mr. Sean Lee 中國移動香港有限公司董事兼行政總裁 — 李帆風先生	China Mobile Hong Kong Company Limited has been a mobile network operator in Hong Kong for years. To address security internally, China Mobile set up a department which is responsible and accountable for IT security administration. The Classroom-type training ensures CMHK employees have a good understanding of company information security policies, procedures and best practices. 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, so those who obtain Email data, for instance, will likely not get their hands on mobile data as well. To address security externally, China Mobile splits customer's data into three into three tiers for better protection: 1) basic client info (i.e. phone numbers, passwords); 2) call detail record; 3) customer behavior (e.g. spending patterns, data package used). As telephone scammers have recently targeted foreign Asians in Hong Kong, one of their primary tactics involves pretending to be a customs agent with the intention of tricking people into believing they have an important parcel that needs to be retrieved. These phone calls tend to come from overseas but have Hong Kong caller IDs. As such, CMHK blocks foreign numbers that appear as HK numbers to reduce the likelihood that victims will fall for them. 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。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。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。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，中國移動香港將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）。 電話騙徒最近瞄準在香港的其他亞洲人仕，騙徒其中一個最基本手法就是假冒海關人員，目的是誘使受害者相信自己有可疑包裹需要處理。這些電話通常來自海外，但卻有香港的來電顯示。因此，CMHK會攔截顯示為香港號碼的外國來電，以減少受害者上當受騙的可能性。
CEO of WTT HK Limited – Mr. Vincent Ma 滙港電訊行政總裁 — 馬惟善先生	WTT HK is a service provider in Hong Kong that invests in high-speed fiber network. They are dedicated to adopting cloud services and providing ICT solutions to specific business needs. Cybersecurity is the core lifeblood of WTT's customers and their own business. WTT's sizable cybersecurity team has the advantage of scale that creates 1) comprehensive understanding of technology available for cybersecurity, 2) in-depth understanding of the client's business to serve their mission-critical needs, 3) a proven track record of addressing cybersecurity needs. These factors together create strong credibility that facilitates trust among clients. Ma notes that a successful data breach can be devastating because of potential supply chain effects. The proliferation of cybercrime has reached the point where cybercrime-as-a-service is now a business; people can hire organized and well-equipped hackers with a whole array of cyber-attacks to hack a given target. Since we are dealing with professional cybercriminals, so we need cyber-security as a service to fight them back. Many businesses recognize the valuable need for cybersecurity, but only 8% of Hong Kong companies employ information security staff, and less than 3% of information security management systems have proper incident response mechanisms. Enterprises are advised to start with general protection towards cybercrime, then consider investing in additional selective cybersecurity for critical needs. 滙港電訊有限公司（WTT）是香港一家投資高速光纖網絡服務供應商。他們專注採用雲端服務並為不同企業提供度身制定的ICT解決方案。網絡安全是WTT的客戶及其業務的核心命脈。WTT網絡安全團隊規模龐大，這規模優勢使他們可以1) 全面掌握廣泛的網絡安全技術，2) 深入了解客戶的關鍵任務需求，3) 對網絡安全需要擁有豐富經驗。這些因素增加其信譽，更促進了客戶的信賴。 馬先生指出，由於供應鏈的潛在效應，所以一次的資料洩漏可具極大破壞性。網絡罪案已醞釀成一種商業服務；不法分子聘請有組織、技術設備精良的黑客，並以一系列網絡攻擊「服務方案」來入侵既定目標。因此我們需要網絡安全服務來反擊這些專業的網絡犯罪分子。許多公司意識到網絡安全的重要性，卻只有8%的香港公司有聘用資訊保安人員，不到3%的資訊安全管理系統設有完善的事故應變機制。建議企業先針對網絡犯罪的一般保護，然後再考慮選擇性投資其他網絡安全措施以滿足重要需要。

Office of the Communications Authority 通訊事務管理局辦公室	The Office of Communications Authority (OFCA) is responsible for governmental telecommunication regulations in Hong Kong. OFCA provides operators with practical guidelines on the security measures for proper operation of public Wi-Fi service and next generation networks. Namely OFCA issued the "Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service" and the "Security Guidelines for Next Generation Networks" to all relevant operators to follow. Further, OFCA has also issued a consumer alert to provide the public with further information about the measure and on precautions to guard against possible caller identity spoofing and telephone scams. Ultimately, they are in view of collaboration with and support of relevant parties including government departments and enforcement agencies, operators as well as other stakeholders are crucial to prevent and combat the abovementioned crimes. 通訊事務管理局辦公室（OFCA）負責管制香港的電訊法規。OFCA為營運商提供有關公共Wi-Fi服務運作和下一代網絡安全措施的實務守則。即OFCA向所有相關營運商發出指引「公共Wi-Fi服務設計、實施、管理及運作的保安指引」和「下一代網絡保安指引」。此外，OFCA還會發出消費者注意事項，向公眾提供有關措施的最新消息以及預防電話詐騙的措施。最後，他們通過合作和支持相關機構，包括政府部門、執法機構和營運商等，甚至其他利益相關者對於預防和打擊上述犯罪事項的重要性。
Co-deputy Chairman of Hutchison Telecommunications Hong Kong Holdings Limited – Mr. Cliff Woo 和記電訊香港控股有限公司聯席副主席 — 胡超文先生	Hutchison Telecom Hong Kong Holdings, and its mobile division 3 Hong Kong, is a mobile communications service provider that offers roaming service under 2G, 3G, and advanced 4G LTE networks. 3 Hong Kong recognizes the value of securing data and employs teams dedicated to keeping data safe. According to Woo, 3 Hong Kong is governed by group level polices on information security and data security in areas such as accountability and access control. Therefore, 3 Hong Kong's built-in protocols ensure that only selected personnel can access sensitive data; reports and warnings are promptly addressed if abnormal data access points are detected. Moreover, all of 3 Hong Kong's customer's data are kept internally and not uploaded on the Cloud to decrease data theft. So far, there have been no confirmed cases of data breach. Many countries require people to register and authenticate their identity – via official IDs or passports – when purchasing SIM cards. Woo supports this idea in principle but stresses the intricacies, policies, and sophistication needed for effective implementation. Creating a database can ease tracking cyber acts but can also put the general public's data at risk, so security measures to prevent the database from being hacked are crucial. Ultimately, any procedure that involves official IDs has to be treated carefully; issues also arise when people lose, or claim to lose, their ID documents. 和記電訊香港控股有限公司旗下的流動通訊業務—3香港是流動通訊服務營辦商，透過2G、3G及先進的4.5G網絡，提供漫遊服務。3香港充分瞭解數據安全的重要性，特別聘請專責團隊保障數據安全。胡先生表示，3香港遵照集團政策，確保資訊和數據在不同領域，例如：問責及存取控制等範疇均得到保障。3香港有嚴謹措施確保只有授權人士才可存取敏感資料，當系統偵測到有不尋常的資料存取情況時，便會立即發出報告和警告。此外，3香港所有的客戶資料均保留在內部，沒有上傳到雲端，從而減低資料被盜的機會。到目前為止，仍未錄得資料外洩個案。 許多國家規定客戶在購買SIM卡時，必需提供身份證或護照以登記和認證。胡先生支持這政策，但他強調必需採用更精密、規範和先進的程序，才可有效地執行政策。建立數據庫可以容易追查網絡行為，但也使公眾的資料置於風險中，因此保護數據庫不受黑客攻擊的安全措施至關重要。任何與身份證明有關的程序必須要審慎對待，當中或需面對用戶遺失或聲稱遺失證件時的問題。

CEO of Hong Kong Cyberport Mangement Company Limited – Mr. Peter Yan

香港數碼港管理有限公司
行政總裁 —
任景信先生

Cyberport's overarching mission is to promote innovation and technology in Hong Kong, as well as to implement new technology to current practices. Cyberport's focus on developing Hong Kong into a smart city enables them to serve as a catalyst for industry development, which consists of six areas as the HKSAR Government set out in its Smart City Blueprint (i.e., Smart Living, Smart Mobility, Smart People, Smart Environment, Smart Economy, and Smart Government). Hence, cybersecurity is an integral part of the digital transformation.

One key initiative Cyberport supports startups is through their Incubation Program. Cyberport's Incubation Program selects three start-ups per year and provides resources that facilitate their growth. With $330,000 and support for two years, those chosen by this Incubation Program receive extensive training and resources in various domains, including implementing A.I. technology, marketing, business plans, the ins-and-outs of public relations, use of Cyberport facilities, networking opportunities, and legal advisory services. Given that cybersecurity is essential in today's digital world, Cyberport treats cybersecurity as a welcoming factor when start-ups apply for funding. However, start-ups who are aware of the need for cybersecurity (and the detrimental effects of not implementing security in their products) tend to prioritize launching their products. Due to differences in priorities, start-ups tend to outsource their cybersecurity needs by adopting existing platform-based tools such as Amazon Web Services. These platforms include affordable yet comprehensive tools, infrastructure, and databases.

數碼港的首要使命是推動香港的創新與科技的發展，以及為推行使用新科技。數碼港專注於將香港發展成為一個智慧城市，使他們能夠成為行業發展的催化劑，其中包括香港特區政府在其智慧城市藍圖所述的六個範疇（即智慧生活、智慧出行、智慧市民、智慧環境、智慧經濟和智慧政府）。因此，網絡安全是數碼轉型的一個重要部分。

數碼港其中一項重點措施就是透過他們的數碼港培育計劃支援初創企業。數碼港培育計劃每年選擇三家初創企業，並提供其發展所需的資源。除了有330,000港元和兩年的支援，培育公司更可獲多項支援及資源，包括落實人工智能、市場推廣、業務諮詢、公共關系細節、使用數碼港設施、參與業界交流活動，拓展網絡及法律咨詢服務。鑑於網絡安全在當今的數碼世界中至關重要，所以，初創公司申請資金時，數碼港會將網絡安全視為評審因素之一。但是，一些了解網絡安全需求（以及產品不採納安全措施的不利影響）的初創企公司往往傾向優先推出其產品。由於考慮不同，初創公司傾向採用一些現成的平台式工具（如亞馬遜網絡服務）來滿足其網絡安全需求。通常，這些平台都是經濟實惠且有綜合性工具、基礎設施和數據庫。

CEO of SmarTone – Ms. Anna Yip

SmarTone
總裁 —
葉安娜小姐

SmarTone is a telecommunications operator in Hong Kong for many years. As an operator, SmarTone places their customer's security as one of their top priorities. As such, SmarTone implements several cybersecurity measures to protect its customers against telephone deception.

Besides monitoring and blocking abnormal IDD calls from overseas, SmarTone's "ST Protect" detects and alerts customers unsafe Wi-Fi connections or man-in-the-middle attacks regardless if users are in Hong Kong or overseas. ST Protect detects and halts abnormal app activities (malicious apps, virus and malware) with patented behavioral analytics and ensures apps only access permitted information. Even when phones are off, ST Protect can continuously run a behavioral engine on customers' smartphone to detect threats. ST Protect has detected 420,000 threats since its launch in 2016.

Another defense measure is SmarTone's app "Call Guard", a hassle-free service that protects customers from unwanted calls without saving the customers' contacts. This feature is especially useful because calls from overseas can be pricey (e.g. roaming fee), and blocking junk calls can deter telephone deception calls.

SmarTone已服務香港多年電訊服務營運商。作為營運商的SmarTone把客戶的安全性作為其首要任務之一，同樣地SmarTone實施多項網絡安全措施，以保護其客戶免遭電話詐騙。

除了監控和攔截異常海外來電外，SmarTone的「ST Protect」無論客戶身處何地，都能偵測和發出警告給客戶一旦有不安全WiFi連接或中間人攻擊出現（Man-in-the-middle attack）。ST Protect採用專利的行為模式分析系統，能偵測異常的程式操作，包括但不限於惡意應用程式、病毒及惡意軟件，確保程式只存取許可的資訊。即使手機處於關機狀態，ST Protect以利用行為模式系統不斷進行威脅檢測。自2016年推出以來，ST Protect已偵察超過42萬次威脅。

另一項防護措施是SmarTone的應用程式「來電管家」，在不需要存取用戶個人通訊錄的情況下，無間斷為客戶阻截滋擾來電，讓客戶免受滋擾。在用戶接聽長途電話的時候，這項功能顯得尤其有用，因為長途電話費可能很昂貴（如：漫遊費用），而且阻截了海外滋擾電話也可減少了電話詐騙來電。

Upcoming Threats in Technology

As technology continues to advance, we need to be cognizant of its accompanying cyber-risks. Namely, we discuss 5G and Internet of Things (IoT), as they are set to take hold in the near future. The next generation of communication network is exciting, but concerns pertaining to cybercrime are sure to follow.

The era of 5G technology aims to create a digital society that penetrates all aspects of life. In addition to increased speed and size, 5G technology includes augmented reality, artificial intelligence in wearable devices connected devices, and virtual reality (Sharma, 2013). These advances bring on countless applications in traveling, medicine, education, and other domains, but open the doors for innovative techniques for cybercrime and security breaches (Ahmad et al., 2018). Concerns include personal privacy, DDoS attacks, bots, roaming security, and compromised company networks. These are important issues to consider as 5G security standardization is yet to be fully developed.

On an individual level, more potent connections also call for more potent security. To secure personal privacy, there must be anonymity-based technology to secure one's data (e.g. encryption) and location-clocking-based (location-cloaking-based) algorithms to conceal one's location (Mantas et al., 2015), and close monitoring of what apps are downloaded and used. As personal smartphones are increasingly brought to one's work environment to access information in company networks, but doing so raises security concerns (Dhingra, 2016). Personal smartphones can compromise a company network by serving as a wormhole to other networks connected to the phone.

On a broader level, future 5G mobile networks can serve as portals for DDoS attacks due to its high connectivity capacity. Hackers or bots can generate and inject large amounts of traffic into networks, infect mobile devices, drain network resources, and lead to service degradation (Mantas et al., 2015). Bots can also cause chaos via DDoS by distributing mass amounts of spam or installing malware.

Besides 5G, we need to consider the risks Internet of Things (IOT) could bring. IOT foresees connectivity of trillions of devices together, but ubiquitous data collection, storage, processing, and transfers can lead to perverse consequences (Ziegeldorf, Morchon, & Wehrle, 2013). Smartphones gather unprecedented amounts of data regarding the owner's activities, locations, and identifiers. These data can be used against the owner if it falls in the wrong hands, known as an inventory attack. When this occurs, hackers can identify, track, and profile their targets with high accuracy. Social engineers can capitalize on inventory information (e.g. speech recognition) to break-in private property, reset one's passwords by knowing the answer to security questions, or manipulate victims with "fake kidnapping" or "pretending official" tactics.

科技將面臨的威脅

隨著科技的不斷發展，我們需要意識到隨之而來的網絡風險。所以，我們要了解5G和物聯網（IoT），因為它們在不久將來會具有舉足輕重的地位。下一代通訊網絡需是令人熱切期待，但與網絡犯罪有關的問題定必接踵而來。

5G時代的技術目標是創造一個貫穿生活各個方面的數碼化社會。除了速度被提升和規模更廣大之外，5G技術也增強了擴增實境（AR）、穿戴式裝置配備人工智能以及虛擬實境（VR）等技術發展（Sharma，2013）。這些進步為旅遊、醫學、教育和其他領域帶來無數的應用，也為打擊網絡犯罪和安全漏洞問題帶來創新技術（Ahmadet et al.，2018）。同時，個人私隱、阻斷服務攻擊、機械人、漫遊安全和公司網絡被攻擊等問題都需要關注，因為現時5G安全性的標準化尚未完全被開發。

在個人層面方面，越來越多重要的連接也需要更穩固的安全措施。為了保護個人私隱，必須要以匿名基礎技術來保護個人的資料（例如：加密）和匿名位置基礎技術來隱藏個人位置（Mantas et al.，2015），並需要密切監控那些應用程式已下載和其使用記錄。個人智能手機逐漸已融入個人工作中並能存取公司網絡中的資料，可是這樣會引發安全性問題（Dhingra，2016）。個人智能手機可以像蟲洞一樣，破壞著公司的網絡。

在廣泛層面方面，未來的5G流動網絡能成為DDoS攻擊的入口，因它具較高的連接能力。黑客或機械人能製造及注入大量流量到網絡中、侵染流動設備、消耗網絡資源，務求導致服務質素下降（Mantas at el.，2015）。分散式阻斷服務攻擊（DDoS）更可以利用機器人，發出大量「垃圾郵件」或安裝惡意軟件務求使目標網絡造成混亂。

除了5G，我們還需要考慮物聯網（IoT）帶來的風險。物聯網預示著萬物可互聯，但少不免存在資料的收集、存儲、處理和傳輸的情況，這些可以引發不良後果（Ziegeldorf、Morchon & Wehrle，2013）。智能手機會收集大量有關用戶的日程、位置和身份識別等資料。如果這些資料落入壞人手中，便會用作攻擊用戶，這稱為庫存攻擊。發生這種情況時，黑客可以準確地識別、跟踪和了解目標資料。社交工程師可以利用庫存中的資料（例如：語音識別）去闖入私人物業、因獲取安全問題的答案，從而重置用戶的密碼，或者通過「虛構綁架」或「假冒官員」手段來操縱受害者。

物聯網隨著不斷改善功能而斷續發展，但立法的腳步卻遲遲還沒有跟上。就怎樣存儲、收集和披露的個人資料方面仍不受法律管制，並且缺乏安全條件協議。當因資料洩漏而發生網絡犯罪時，責任問題就會變得複雜。

IOT is still evolving with changing features while legislation is not keeping up. How people's data is stored, collected, and disclosed is not legally regulated. There also lacks protocols for security requirements, which complicates how cybercrimes can be prosecuted if there are issues of data leaks.

In the 5G system, there are new security risks related to software and hardware implementation aspects in virtualized network infrastructure supporting virtualized network functions, network slicing, Service-Based Architecture (SBA), communication between applications, communication between virtualized network functions, and APIs. As a consequence, in order to address the security risks in 5G End to End architecture, in addition to the traditional network security approach based on protecting communication channels and protocols, a holistic approach, involving also computer security and cybersecurity aspects, is needed. Security sub-group in different organizations such as the Next Generation Mobile Network Alliance (NGMN, www.ngmn.org), and the 3rd Generation Partnership Project (3GPP, www.3gpp.org) have been working to identify, make standards and recommendations to tackle new threats and security issues that may arise with 5G.

Machine learning is an effective tool that can be employed in many areas of information security such as authentication systems, evaluating the protocol implementation, assessing the security of human interaction proofs, and smart meter data profiling. There exist some robust anti-phishing algorithms and network intrusion detection systems. However, the machine learning classifiers themselves are also vulnerable to malicious attacks. There has been some work directed to improving the effectiveness of machine learning algorithms and protecting them from diverse attacks (Ford et al., 2014).

在5G系統中，虛擬化網絡基礎設施於虛擬化網絡功能、網絡切片、服務基礎架構（SBA）、應用程式之間的溝通、虛擬化網絡功能之間的溝通以及APIs提供支援，但其軟件和硬件實施方面出現了新的安全風險。因此，為了解決5G端到端架構中的安全風險，除了基於保護通訊渠道和協議的傳統網絡安全規條外，還需要一些涉及電腦安全和網絡安全兩方面的整體規條。下一代流動網絡聯盟（NGMN，www.ngmn.org）和第三代合作夥伴計劃（3GPP，www.3gpp.org）等不同組織的安全小組一直在努力就身份識別、制定標準和建議來解決5G帶來新的威脅和安全問題。

機器學習是一種有效的工具，可應用於許多資料安全領域，例如：認證系統、評估協議實施、評估人類交互證明的安全性以及智能儀表的數據分析。同時，也是一個強大的反網絡釣魚運算工具和網絡入侵檢測系統。但是，機器學習始終容易受到惡意攻擊。一些改善機器學習效率及免受各種攻擊的工作已經遂一展開（Ford et al，2014）。

打擊網絡犯罪和電話騙案的最佳實踐

當一個人使用虛擬領域時，便逃不過遇上網絡犯罪的風險。我們能怎樣保護自己免受網絡犯罪攻擊呢？我們以幾個打擊網絡犯罪及電話詐騙的最佳實踐作結尾。

首先，要意識到網絡犯罪的無處不在和潛在力。將科技融入生活各項需要的同時也讓網絡犯罪蔓延到我們的生活裡。如WTT的馬惟善先生所指，如果設備連接到其他設備，網絡黑客可能會產生連鎖反應。受到攻擊的智能手機可能會影響到個人的網上帳戶、

Best Practices to Combat Cybercrime and Telephone Deception

Given the inevitable risks of cybercrime when one participates in the virtual realm, how do we best protect ourselves from cybercrime? We close with several best practices to combat cybercrime and telephone deception.

Foremost is realizing the omnipresence and potential for cybercrime. Incorporating technology to virtually all aspect of one's life opens the potential for cybercrime to creep into all aspects of one's life. As mentioned by Mr. Vincent Ma of WTT HK, cyber hacks can have ripple effects if devices are connected to other devices. A smartphone that is compromised could affect one's online accounts, calendar, Emails, text messages, etc. because businesses live within an ecosystem of other businesses, such that data breaches not only impact one company but also exposes data from business partners.

To address this, we need mass education about cybercrime, as echoed by our interviewees. Mr. Bernard Lee of BlueSky believes that cyber education is essential for everyone's safety and we have the responsibility to keep others safe. Ms. Gabriela Kennedy of Mayer Brown said we should be cautious, resist social engineering, and verify the identity of the caller before giving away information. The police interviewees advocate communicating with close ones about experiences regarding any form of cybercrime and telephone deception. Mr. Sean Lee of China Mobile argues that the decline of telephone deception is largely dependent on the user's awareness of deception tactics.

Besides education, individuals should practice better security measures. Many young people still share their passwords with others (Meter & Bauman, 2015), and it is up to adults to ensure this does not happen. As mentioned by Mr. Stephen Ho of CITIC Telecom, we should practice easily-implemented procedures such as cloud backup and two-factor authentication. These may include downloaded apps that blocks blacklisted numbers, such as SmarTone's "call guard", as mentioned by Ms. Anna Yip of SmarTone.

We all have the right to access information in the Cyber world without fear of being hacked and attacked. We all want to be free from deception and threat. "Freedom, in any case, is only possible by constantly struggling for it" – Albert Einstein.

日曆、電子郵件、短訊等，再者會因企業之間之聯繫，使資料洩露不僅會影響一家公司，還會披露相關合作夥伴的資料。

為了打擊網絡犯罪，我們需要進行大規模的教育工作，這也正正是我們受訪者所建議的。藍天的李本立先生認為，網絡教育對每個人的安全至關重要，我們有責任維護他人安全。孖士打律師行的甘乃迪女士認為，資訊科技界應該繼續教育他們的客戶以及大眾，錄製自家視頻或專頁網站去提供有關詐騙行為和詐騙電郵的線索和特徵。我們必須小心謹慎、抵抗社交工程，並確認來電者身份後才可提供個人資料。警方提倡市民應該與親友多交流各種有關網絡罪案的手法。中國移動的李帆風先生認為，要降低電話詐騙個案，主要取決於用戶對欺騙手法的意識。

除了普及教育，個人應該採用較好的安全措施。許多年輕人仍然會將密碼告知他人（Meter＆Bauman，2015），但成年人就絕對不可再有這種情況發生。正如中信國際電訊CPC的何偉中先生所說，我們應該採取易實施的程序，例如：雲備份和雙重身份驗證。另外，如SmarTone的葉安娜小姐所述，SmarTone的來電管家是可阻截滋擾來電的應用程式。

我們每個人都有權在網絡世界中無懼無畏地瀏覽資訊。我們每個人都希望擺脫詐騙與威脅。「不管如何，自由是自己爭取的」—阿爾伯特愛因斯坦。

References
參考文獻

Acton, A. (2017, July 13). How To Stop Wasting 2.5 Hours On Email Every Day. Retrieved from https://www.forbes.com/sites/annabelacton/2017/07/13/innovators-challenge-how-to-stop-wasting-time-on-emails/#470041539788

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine,2(1), 36-43.

Burg, N. (2013, December 11). UnifyVoice: How Technology Has Changed Workplace Communication. Retrieved from https://www.forbes.com/sites/unify/2013/12/10/how-technology-has-changed-workplace-communication/#67aaebe1670b

Chiluwa, I. (2009). The discourse of digital deceptions and '419' emails. Discourse Studies,11(6), 635-660.

Daitch, H. (2018, July 06). 2017 Data Breaches - The Worst Breaches, So Far | IdentityForce®. Retrieved from https://www.identityforce.com/blog/2017-data-breaches

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior,26(6), 1739-1747.

Detardo-Bora, K. A., & Bora, D. J. (2016). Cybercrimes: an overview of contemporary challenges and impending threats. In J. Sammons (Ed.), Digital Forensics (pp. 119-132). Boston, MA: Syngress.

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). Procedia Computer Science,78, 179-184.

Fisher, M., Goddu, M. K., & Keil, F. C. (2015). Searching for Explanations: How the Internet inflates estimates of internal knowledge. Journal of Experimental Psychology: General,144(3).

Ford, Vitaly & Siraj, Ambareen. (2014). Applications of Machine Learning in Cyber Security. 27th International Conference on Computer Applications in Industry and Engineering, CAINE 2014.

FTI Consulting. (2015). Countering the growing threat of cyber blackmail. Retrieved from http://ftijournal.com/article/countering-the-growing-threat-of-cyber-blackmail

Gianvecchio, S., Xie, M., Wu, Z., & Wang, H. (2008). Measurement and classification of humans and bots in Internet chat. 17th USENIX Security Symposium.

Goldman, K. D., & Schmalz, K. J. (2006). "CSI: Mylaptop": Computer security issues: How vulnerable am I? Health Promotion Practice,7(3), 276-279.

Guo, L., Trueblood, J. S., & Diederich, A. (2017). Thinking fast increases framing effects in risky decision making. Psychological Science,28(4), 530-543.

Hamilton, K. A., McIntyre, K. P., & Hertel, P. T. (2016). Judging knowledge in the digital age: The role of external-memory organization. Applied Cognitive Psychology, 30(6), 1080-1087.

Hancock, J. T. (2007). Digital deception. In Oxford Handbook of Internet Psychology (pp. 289-301). Oxford Library of Psychology.

Hong, J. (2012, January 01). The state of phishing attacks. Retrieved from https://cacm.acm.org/magazines/2012/1/144811-the-state-of-phishing-attacks/fulltext

Iannone, N. E., Mccarty, M. K., & Kelly, J. R. (2016). With a little help from your friend: Transactive memory in best friendships. Journal of Social and Personal Relationships, (6), 1-21.

Jacobson, B., & Donatone, B. (2009). Homoflexibles, omnisexuals, and genderqueers: Group work with queer youth in cyberspace and face-to-face. Eastern Group Psychotherapy Society,33(3), 223-234.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies,63(1-2), 203-227.

Kaspersky Lab. (2013). Kaspersky security bulletin 2013. Retrieved from https://report.kaspersky.com/

Lokot, T., & Diakopoulos, N. (2015). News bots: Automating news and information dissemination on Twitter. Digital Journalism,4(6), 682-699.

Mantas, G., Komninos, N., Rodriuez, J., Logota, E. & Marques, H. (2015). Security for 5G Communications. In: J. Rodriguez (Ed.), Fundamentals of 5G Mobile Networks. (pp. 207-220). John Wiley & Sons, Ltd.

Mckenna, K. Y., & Bargh, J. A. (1998). Coming out in the age of the Internet: Identity "demarginalization" through virtual group participation. Journal of Personality and Social Psychology,75(3), 681-694.

Mims, C. (2012, October 22). A surprisingly long list of everything smartphones replaced. Retrieved from https://www.technologyreview.com/s/428579/a-surprisingly-long-list-of-everything-smartphones-replaced/

Mitchell, K.J., & Johnson, M.K. (2000). Source monitoring: Attributing mental experiences. In E. Tulving & F.I.M. Craik (Eds.), Oxford Handbook of Memory (pp. 179-195). New York: Oxford University Press.

Mitnick, K. D., & Vamosi, R. (2017). The art of invisibility: The worlds most famous hacker teaches you how to be safe in the age of Big Brother and big data. New York: Little, Brown and Company.

Naquin, C. E., Kurtzberg, T. R., & Belkin, L. Y. (2010). The finer points of lying online: E-mail versus pen and paper. Journal of Applied Psychology, 95, 387-394.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of persuasion. Communication and Persuasion, 1-24.

Pulman, A., & Taylor, J. (2012). Munchausen by Internet: Current research and future directions. Journal of Medical Internet Research,14(4).

Ratkiewicz, J., Conover, M. D., Meiss, M., Goncalves, B., Flammini, A., & Menczer, F. (2011). Detecting and tracking political abuse in social media. Proceedings of the Fifth International AAAi Conference on Weblogs and Social Media.

Robertson, A. (2017, May 03). Google Docs users hit with sophisticated phishing attack. Retrieved from https://www.theverge.com/2017/5/3/15534768/google-docs-phishing-attack-share-this-document-with-you-spam

Romano, A. (2018, March 20). The Facebook data breach wasn't a hack. It was a wake-up call. Retrieved from https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained

Rosenfield, M. (2016). Computer vision syndrome (a.k.a. digital eye strain). Optometry in Practice,17(1), 1-10.

Sharma, P. (2013). Evolution of mobile wireless communication networks-1G to 5G as well as future prospective next generation communication network. International Journal of Computer Science and Mobile Computing,2(8), 47-53.

Sparrow B, Liu J, Wegner DM. Google effects on memory: Cognitive consequences of having information at our fingertips. Science. 2011;333 :776-778.

Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior,7(3), 321-326.

Tamir, D. I., Templeton, E. M., Ward, A. F., & Zaki, J. (2018). Media usage diminishes memory for experiences. Journal of Experimental Social Psychology,76, 161-168.

Ward, A. F. (2013). One with the cloud: Why people mistake the Internet's knowledge for their own. Cambridge, Massachusetts: Harvard University Unpublished doctoral dissertation).

Ward, A. F., Duke, K., Gneezy, A., & Bos, M. W. (2017). Brain Drain: The mere presence of one's own smartphone reduces available cognitive capacity. Journal of the Association for Consumer Research,2(2), 140-154.

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. Criminology & Criminal Justice,16(2), 176-194.

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. Computer Fraud & Security,2018(1), 15-20.