Educate the Public to Defend against Cybercrime
教育公眾防範網絡罪案

Interviewed by : Mr. Alex Tam
採訪者：譚永耀先生

Ms. Gabriela Kennedy
Partner
Mayer Brown
甘乃迪女士
合夥人
孖士打律師行

The rapid rate of technology adoption brings countless benefits to societies and its citizens. However, adopting technology also brings advanced technical information that is mostly unknown to the general public. 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 Hong Kong citizens do not utilize the full potential of technology. Though we cannot attribute cause and effect, there is a strong correlation between citizens who do not utilize technology to its capacity and citizens who are not aware of the latest tactics in cybercrime, which subsequently makes them vulnerable targets for cybercriminals. Kennedy discussed key tactics in cybercrime, some aspects that make cybercrime unique in Hong Kong, and how the IT industry can help combat cybercrime.

Latest Tactics in Cybercrime

Social Engineering. Cybercrime has proliferated in recent years partly due to sophisticated social engineering, which is the practice of using various psychological tactics to trick victims into giving away their personal information. Initially, social engineering began with fictitious bank sites when Internet banking started, which in turn promulgated two-factor authentication. Later, social engineering turned to target corporations with less sophisticated security systems and trained workforce who are well equipped with detecting intrusions. Today, social engineers can capitalize on their targets' social media to learn the patterns, lifestyle, and habits of their targeted persons. As a result, many corporations enact strict policies that dictate what employees can or cannot post on social media sites. Senior executives, for instance, are not allowed to post where they are on a business trip because it gives away valuable context for social engineers.

科技的迅速普及給社會和市民帶來無數好處。然而，採用科技也帶來了普羅大眾所不認識的嶄新技術資訊。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。雖然我們不能將原因和結果歸為一類，但在不充分利用科技的市民和不了解網絡罪案最新策略的市民之間存在著很強的關聯性，從而使他們成為易受網絡犯罪分子攻擊的目標。甘乃迪女士談論了打擊網絡罪案的主要策略、一些令香港網絡罪案與眾不同的因素，以及資訊科技界如何可以協助打擊網絡罪案。

網絡罪案的最新手法

社交工程。近年來，網絡罪案激增，部分原因是來自先進的社交工程，即利用各種心理手段誘使受害者洩露個人資料。最初，當網上銀行開始時，社交工程的矛頭指向虛擬的銀行網站，所以研發出雙重認證。後來，社交工程的目標轉向了那些缺乏先進安全系統和網路安全專員的公司。如今，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。因此，許多公司製定了嚴格的政策，規定那些內容員工可以或不可以在社交媒體網站上發布。例如，不允許高級行政人員在出差地點發帖，因為這給社交工程師提供了寶貴的背景資料。

虛假招聘啟事。網絡罪案的一個創新策略是，網絡犯罪分子自稱是X公司，代表X公司發布廣告招聘員工，待求職者發送簡歷時收取費用。雖然費用本身並不高（比如50美元），但這種欺詐行為可能會損害網絡犯罪分子所冒充的合法公司的聲譽。

Fake Job Listings. A creative tactic of cybercrime involves cybercriminals – claiming to be company X – posting job ads looking to hire employees on behalf of company X. However, sending in a CV requires a submission fee. Though the fee itself is not large (e.g. US$50), the fraud may damage the reputation of the legitimate company that the cybercriminals impersonate.

Identity Theft. Kennedy has dealt with many significant cases in the past couple of years that revolve around the theft/leakage of personal data, averaging to roughly two cases per month. Hackers tend to target companies with massive databases that contain customer information all of it very valuable, including the customer's credit card information, payment information, mobile phone number, residence address, or anything else that assists hackers in identity theft. Personal data is often sold off on the dark web.

Smartphone Apps. Kennedy notes that many apps that appear legitimate or connected to or sanctioned by legitimate businesses collect personal information. App stores lack a vetting and filtering process that would weed out the bad actors. There are many so called "medical apps" that may look as if they were sanctioned by medical insurance companies when in fact that is not the case. Volunteering information about one's health on such apps is a sure way to having one's data sold to the highest bidder.

Kennedy also highlighted the risk of using unsecured Public Wi-Fi networks when working on confidential documents and also the dangers of accepting "USB Open Wi-Fi systems" – in coffee shops and hotels for example – invite trouble. Apple devices which connect to the vulnerable Wi-Fi can see other Apple devices connected and can easily see what these other devices are doing.

Public Surveillance. Some countries such as the U.K. have CCTV cameras installed in public areas, and these cameras are equipped with advanced technology that can not only identify people from a distance, but also has the ability to recreate one's biometrics. If compromised, hackers can learn of their target's whereabouts and lifestyle.

USB Drives. A small USB device can carry malware that infect computers once the USB is plugged in. Kennedy mentioned that one way cyber security staff test the preparedness of a company is to have person X drop a "corporate gift" – usually a USB drive – to the receptionist and have the receptionist deliver it to person Y because they just had a meeting together and person X forget to leave person Y a gift. Kennedy states that the company's data can be jeopardized within the hour that the USB is plugged into the operating system. This anecdote displays the vulnerability that systems have when faced with malicious software, even something as small as a flash drive can prove to be an easy way to gain access to a company's computer system.

身份盜竊。在過去的幾年裡，甘乃迪女士處理過許多與盜竊/洩露個人資料有關的重大案件，平均每月大約有兩宗個案。黑客傾向於將目標對準擁有大規模數據庫的公司，這些數據庫包含客戶非常有價值的資料，包括客戶的信用卡資料、付款資料、手機號碼、住所地址，或其他任何有助於黑客竊取身份的資料。個人資料經常在黑網上被廉價出售。

智能手機應用程式。甘乃迪女士指出，許多看似合法、與合法企業有關聯或得到合法企業認可的應用程式都會收集個人資料。應用程式商店缺乏用來剔除不良行為的審查和過濾程序。有很多所謂的「醫療應用程式」，看起來好像是獲醫療保險公司所批准，但實際上並非如此。在這些應用程式上自願提供自己的健康資料，相等於讓他們將自己的數據賣給出價最高的不法分子。

甘乃迪女士還強調了使用不安全的公共Wi-Fi網絡的風險，在處理機密文件以及在咖啡店和酒店接受「USB開放Wi-Fi系統」也有機會帶來麻煩。「蘋果」設備連接到易受攻擊的Wi-Fi系統時可以看到同時連接到該系統的其他「蘋果」設備，也很容易地看到其他「蘋果」設備在做什麼。

公眾監察。一些國家如英國在公共場所安裝了閉路電視攝像鏡頭，這些攝像鏡頭配備了先進的技術，不僅可以遠距離識別人，還能重塑該些人士的生物特徵。一旦入侵成功，黑客就可以了解目標的行踪和生活方式。

USB驅動器。一個小型的USB設備可以儲存著惡意軟件，一旦插入USB，電腦就會受到感染。甘乃迪女士提到一種網絡安全人員測試公司防備情況的方法是讓X先生放下一份「企業禮品」（通常是USB驅動器）給接待員，讓接待員把它轉送到剛于X先生開完會的Y先生， X先生聲稱自己忘了把該禮物送給Y先生。甘乃迪女士表示，公司的數據可能會在USB插入操作系統的一個小時內被損害。這則趣聞表明了企業系統在面對惡意軟件入侵時的脆弱性，證明即使是像閃存驅動器這樣小的東西很容易便能入侵企業的電腦系統。

香港的網絡罪案

香港在針對網絡罪案或網絡安全的立法方面頗為落後。我們可以從其他國家採用的方法中作參考，比如製定官方的電腦犯罪法規。香港有多項用來處理網絡罪行的法律條文（例如《通訊條例》、《刑事罪行條例》），但這些法律條文略顯零散。這些零散的規定存在問題，因為網絡罪犯可以利用公司的供應鏈獲取敏感數據;在一個前哨站中發生的數據洩露可能危及一系列系統。此外，公司在各自的供應鏈內的安全問題上往往缺乏協調。根據《個人資料私隱條例》，香港沒有強制通布資料洩

Cybercrime in Hong Kong

Hong Kong is lagging behind when it comes to legislation aimed at cyber crime or cyber security. The city could benefit from adopting practices developed in other countries, such as having an official computer crimes statute. Hong Kong has many provisions (e.g. communications ordinance, crimes ordinance) that deal with cybercrime, but these provisions are somewhat patchy. Scattered provisions are problematic because cybercriminals can obtain sensitive data by exploiting a company's supply chain; data breaches that occur in a single outpost can imperil a string of systems. Furthermore, companies are often lacking in coordination with regards to security matters within their respective supply chains. Hong Kong does not have a mandatory data breach notification under the personal data privacy ordinance. Without clear data breach regulations, the fallback for regulators is to make companies accountable for the security of their data. Weak enforcement powers and sanctions in the event of a breach are unlikely to focus the mind on tightening the grip on the supply chain and implementing strong security. Cybercrimes that target Hong Kong citizens but are perpetrated by actors located overseas (e.g. telephone deception calls from overseas) can at times prove difficult to handle. Although public directories – physical or digital – list personal information for a particular purpose (e.g. emails and phone numbers listed for work purposes), social engineers can use this information for other purposes (e.g. to impersonate officials and obtain goods/money by deception). When overseas social engineers use personal information to perpetrate fraud it becomes difficult to punish those responsible and to obtain the necessary evidence for a prosecution in Hong Kong. Nevertheless, it is still possible to trace back where data is sent, but all this takes time and money. For email scams, the directors and managers in a company have the right to gain access to all employees' emails if it is necessary to solve cases of cybercrime (e.g. phishing scams). For money and data transfers, insurance companies can do forensics on every single log to determine where the intrusion occurred.

Due to the fact that we are living in an increasingly technologically dependent society, cyber attacks are of fundamental concern, therefore spending money on IT and cyber security is crucial in assuring the online safety of individuals. The issue arises when small-to-mid enterprises with limited resources face the dilemma of deciding how much to invest in cyber security. An NGO who has their website hijacked, for instance, might need to find external parties for help on a pro-bono basis.

IT Industry Should Educate the General Public

IT companies could choose to invest in IT security experts and related parties to develop their own training materials – targeting both their workforce and their customers. The purpose of such training is to inform the public how to detect a cyber-breach or an intrusion attempt, the clues, hallmarks, of malicious online behaviour. Videos can educate the public by highlighting case studies such as the fake job listing case mentioned above that used a Gmail account to accept CVs. These videos can inform the public that no large corporation would accept CVs via

露的規定。在沒有有關資料洩露的明確規定的情況下，監管機構的應變方法是讓企業對其數據的安全性負責。由於執法權力和製裁力度軟弱，在資料洩露的情況出現時，注意力就無法集中在加強對供應鏈的監管和實施牢固的安全措施上。一些以香港市民為目標，但由海外假扮者（例如，來自海外的電話詐騙來電）所犯下的網絡罪案顯然難以處理。雖然實體或數碼形式的公共目錄已列明個人資料的特定用途（例如為了工作目的而列出的電郵地址和電話號碼列出的），社交工程師却利用這些資料而作其他用途（例如，假冒某官員和以欺騙手法獲取商品/ 金錢）。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。對於電郵詐騙，若有需要解決網絡犯罪案件（如網絡釣魚詐騙），公司董事和經理有權讀取所有員工的電子郵件。對於金錢和資料轉移，保險公司可以對每項交易進行鑑證，以確定入侵在哪裡發生。

由於我們生活在一個越來越依賴科技的社會，網絡攻擊帶來了基本的憂慮，因此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。例如，當非政府組織的網站被入侵時，他們可能需要尋求外來機構的免費協助。

資訊科技界應該教育大眾

資訊科技公司可以選擇投資於聘請資訊科技安全專家和有關人士，以開發自己的培訓材料－既針對員工，也針對客戶。這種培訓的目的是告訴公眾如何發現網絡攻擊或入侵企圖、惡意網絡行為的線索和特徵。視頻可以通過突出案例研究來教育公眾，比如上面提到的使用Gmail賬戶來接收簡歷的虛假招聘啟事案例。這些視頻可以告訴公眾，沒有知名企業會通過Gmail賬戶來接收簡歷。另一方面，資訊科技公司也可以設立網站為網絡罪案受害者提供匿名討論區，讓他們分享自己的經歷，以免其他人同樣地受騙。然而，這些視頻或網站也可能受到網絡犯罪分子的監視，促使他們想出層出不窮的方法來欺騙受害者。網絡犯罪分子也可以在討論區上留言，以迷惑讀者。通過這些方法，企業可以教育公眾關於網絡罪案的惡意本質，在一個被科技包圍的世界裡，這些知識將有效減低網絡罪案在我們社會中的惡性影響。

結語

甘乃迪女士提倡為公眾提供更多的網絡教育。那些提供「好得難以置信」的商品或服務的電子郵件或電話大概是「好得難以成真」。她建議提供更多有關網絡罪案新趨勢的資料，讓人們在洩露個人資料之前保持克制。

Gmail accounts. The websites, on the other hand, could host an anonymous discussion board for cybercrime victims to share their experiences so others would hopefully not be duped in the same way. However, these videos or websites would likely be monitored by cybercriminals as well, thereby motivating them to come up with novel ways to scam victims. Cybercriminals could add their comments to the discussion board to confuse readers as well. Through these methods, corporations can educate the general public on the malevolent nature of cybercrime, and in a world where we are surrounded by technology this knowledge is crucial in minimizing the malignant effect of cybercrime in our society.

Concluding Remarks

Kennedy advocates more cyber education for the general public. Emails or telephone calls that offer goods or services that seems "too good to be true" are "probably too good to be true". She recommends making more information available on new trends in cybercrime and for people to exercise more restraint before divulging personal information.