守望牧職
香港基督徒學會
Hong Kong Christian Institute
04
香港九龍旺角塘尾道54-58號永利工業大廈9樓901室 | 2398-1699 | info@hkci.org.hk / www.hkci.org.hk
第4期2022.1 督印人：龔立人 主筆：何嘉衡

資訊安全隱患

何嘉衡
研究及出版幹事

前言

時至今日，絕對不會有人否定資訊科技的重要性，因為人類生活的每一方面都會看到資訊科技的身影。最普遍的現象大概是人們以智能手機接收資訊、娛樂、消費、工作等，甚至有些人在生活中只用平板電腦 (tablet) 和智能手機，這樣電腦也「慳返」。在智能裝置早已取代電腦成為當代人最重要的資訊科技設備的今日，智能電話理所當然地成為日常生活不可或缺的一部分。不過在人類社會和生活模式都被智能裝置大幅度改變面貌的同時，很多人都沒發現自己正身處一個與以往歷史很不一樣的時代，在這個時代裡每個人都需要面對前所未有的問題與危險，那就是與資訊安全相關的問題。

資訊安全的意思，是一套安全機制用來保護電腦系統、網路、應用程式和容器等各類資訊技術的完整性，防止遭受攻擊、破壞，以及未經授權的存取動作；以保護使用者的數位資料不被外洩和盜用。

個人、公司或政府資訊洩漏所帶來的後果，小則是導致身分被冒用、信用卡被盜用等問題；大則是導致企業龐大損失，甚至影響一國的運作，例如發電廠、輸油管等設施被黑客攻擊。絕非筆者危言聳聽，這些新聞確實經常在日常世界中聽聞。雖說資訊安全漸漸因為智能產品在人們日常生活中普及而變得更為重要，不過按筆者在日常生活中的觀察，不少人仍然經常掉以輕心，實在令人替他們擔心。本期《守望牧職》正要從資訊安全的角度出發，與讀者一同探討使用者在資訊安全上可以有多大程度的自我保障，以致既不會過於恐懼自身對資訊科技的無知和不足，亦不會對相關的安全問題過於掉以輕心，並且成為更好而且負責任的「數碼公民」。

萬物都能上網的時代已經到來

可能很多人沒有意識到，今時今日已經愈來愈多器材和工具能夠連接互聯網；除了理所當然的電腦和智能手機，還包括沒有想像過有需要「上網」的用品，如雪櫃、手錶、咖啡機等。連本來沒必要上網的物件也要接上互聯網，在某些論者的眼中代表著「物聯網」時代（Internet of Things）已經到來：人們「在電腦上加裝各式用品。隨著電腦愈來愈小巧實惠，內嵌電腦的物品也愈來愈多。」[1] 物聯網除了顯示網絡技術的進步，也代表電腦技術的進步。因為雖然可以連接網絡的物件原本的用途並非運算，也並非接連互聯網，但是當生產者將電腦運算與連接網絡功能附加進去那些物件，那些物件也變成廣義上的電腦。[2]

很多原因都造就物聯網時代的到來。除了目前的晶片技術令電腦的體積可以愈來愈細小[3]，主要原因是在互聯網技術發展一日千里的情況下，互聯網變得可以快速傳送大量數據，因此讓雪櫃「上網」非但不會霸佔電話通話[4]，不會使其他物件上網速度變慢，還可以增添方便用家的功能。例如可以與手機連接觀看雪櫃內的狀況；可以在雪櫃門外的電子顯示屏使用跨平台的電子月曆，用以記錄食

物的食用日期；甚至已有智能雪櫃能透過人工智能技術，在顯示屏提醒使用者重購已經用完的食材，或提供與雪櫃內的食材相關的食譜等等。除了雪櫃，還有很多日常生活的物件，都已經可以透過互聯網連接，並用智能手機遙距控制，例如寵物的玩具、協助保安的監視鏡頭、室內溫度調節系統等等。

不過，在日常生活各種物件都漸漸「電腦化」的同時，人們沒有警覺它們不再是物件「咁簡單」，因而忽視了與電腦相關的資訊安全；以致擁有相關黑客技術的人，能夠透過網絡攻擊各樣物件。因此，有論者認為在物聯網的時代裡，「電腦安全性會左右一切的安全性，電腦安全性的教訓將可適用在任何地方。就電腦而言，我們最清楚的一點是，無論電腦是汽車、變電所或生物印表機，都容易受到業餘愛好者、行動主義分子、罪犯、民族國家 (編按：Nation State) 和具有科技知識的任何人士攻擊。」[5]

輕視資訊安全的例子

目前不少國家和地區的數碼知識落差非常大，甚至在同一個地方，有人擁有極為先進的資訊科技技術，可以攻擊程式和系統的漏洞來獲取利益（不論是合法或非法）[6]；但也有人只懂得簡單的電腦或智能手機操作，又或是沒有足夠的資訊安全常識，讓個人有電腦裝置的物件暴露在危險之中，更有機會因而蒙受各種程度的損失。

在目前的網絡世界裡，除了個人資訊很容易被竊取和盜用，各式各樣的集團和群體也會遭遇事故、意外和攻擊。例如有大型社交媒體因意外或網絡攻擊而洩漏用戶的個人資料；企業遭黑客入侵並盜取資料；國家基礎建設電腦系統受到攻擊而需要暫停運作等等。這些例子都反映了當今人類一邊享受互聯網和資訊科技進步帶來的方便，但同時亦分分秒秒在面對無所不在的網絡攻擊。甚至美國總統拜登曾公開宣稱，將來大國間爆發熱戰（編按：荷槍實彈的戰

爭），最有可能就是因為遭到外國黑客攻擊而作出反擊。[7]

在討論沒有妥善保護個人資料之前，筆者先舉一個例子來說明，資訊安全與一些刑事案件的可能關係。相信近年在香港生活的人，都試過收到「3」字頭的來電，打來的十居其九是美容廣告或借貸廣告。這些只要不予理睬的廣告來電尚算無害，只是對「嫌麻煩」的人來說，常常接到這些電話還是會感到困擾。而當中真正令人困擾又帶點恐慌的，是來電者會聲稱自己是中國官方單位職員或香港本地銀行職員，並要求接電者提供信用卡或戶口密碼作查核戶口賬目之用；又或是為某些在內地發生的刑事案件交付保證金。雖然香港政府、金融管理局和本地銀行均多次澄清這些是詐騙電話，勸籲市民不要輕易將重要的個人資料告知來電者，或按要求轉賬到對方提供的銀行戶口，以免遭受財物上的損失；但仍然不時會有人墮入騙徒陷阱，損失巨額金錢。[8]

筆者也留意到近期有人在社交媒體表示騙徒能夠清楚說出接電者的全名、身分證號碼和電話號碼，因而險些被騙；最後只是憑對方不是操流利廣東話，以及陳述之事件並沒有發生而識破騙局。[9] 這兩個例子都有個共通的疑問：為什麼騙徒能夠掌握香港人的個人資料？明顯是個人資料遭洩漏了。相關的分析顯示，原因主要分成兩種，一是收集個人資料的公司內部有人不合法地販賣資料給其他機構[10]，又或者有些人曾經在網絡上留下詳細的個人資料，因意外而洩漏或遭黑客竊取。

由於近年各地政府保障個人資料的法規日漸完善，部分販賣個人資料的商業行為已經定性為罪行。例如香港已於2012年修訂《個人資料（私隱）條例》，規管公司或個人於未經個人同意而銷售或轉移個人資料用作圖利，或導致當事人蒙受財產上的損失，最高刑罰可達監禁五年及罰款一百萬；這罰則在一定程度上起到阻嚇作用。[11] 時至今日，大型網絡服務供應商洩漏用戶個人資料的問題，

早已比銀行或保險業者銷售個人資料來得嚴重；因為這些大型網絡服務供應商通常是跨國公司，在全世界擁有極多的用戶。2021年4月美國傳媒Business Insider報導，全球有超過5億Facebook用戶的個人資料，包括電話、電郵、全名等在黑客論壇被公開，疑似是被洩漏的緣故，當中可能涉及300萬個香港用戶。[12]

近年興起的網絡購物也是其中一種洩漏資料的途徑。特別在2019年底因肺炎疫情爆發，不少人都減少外出購物轉而網購的情況下，購物網站很多時會為了方便消費者，而將帳號與信用卡連結；這樣款項會自動在連結的信用卡帳號中扣除。銀行一般都會要求消費者再以短訊收取的認證碼來完成交易，而網絡購物平台也會在交易完成後，以電郵或短訊的方式通知消費者；所以在一般情況下，不法之徒難於盜取購物網站的帳號來直接購物。不過假若允許網絡購物供應商儲存個人資料，例如全名、手提電話或信用卡號碼，就有可能讓黑客從中偷取重要的個人資訊。此外，有些可能大眾不留意，亦不是經常會用到的網絡服務，也有機會洩漏個人資料；例如部分需實名認證的網絡促銷活動，甚至是2020年初部分能入口口罩的公司舉辦「抽口罩」活動[13]，也可能是個人資料洩漏的缺口。

另一個大眾會意想不到的例子是，今年6月，美國著名遊戲製作公司Electronic Arts (簡稱EA) 傳出被黑客盜取超過750GB資料，當中包括在全球各地均非常受歡迎的足球遊戲 FIFA 21和第一身射擊遊戲Battlefield。涉案的黑客更揚言能夠修改往後該遊戲公司出產的遊戲內容，並且利用系統漏洞更改新發行的遊戲。[14] 這次的黑客入侵事件，雖然沒有玩家受害，但遊戲公司可算是蒙受極大損失，因為資料外洩的遊戲是該公司的皇牌遊戲，公司從中取得的利潤極高。後來有報導指出，黑客所以能入侵該遊戲公司的伺服器，是因為有員工於疫情期間在家工作，在登入公司製作遊戲的伺服器時資料外洩，因此黑客得以入侵該遊戲公司開發遊戲的伺服器，並且竊取遊戲的資料。[15] 疫情未發生之前，不少需要使用互聯網進行業務或協

助生產的公司，都會在旗下辦公室使用極為高度設防的電腦，以免資訊外洩或遭黑客入侵。但在疫情之下，在家工作成為了不少人的工作常態，這時候個人的網絡安全和資訊安全，即成為這些公司的極大挑戰。若處理不當，便會像EA一樣招致嚴重損失，甚至可能影響公司未來的發展計劃和營收（營業額）。

資訊安全危及國際關係

網絡攻擊與資訊安全問題，甚至可能會造成國際關係緊張。今年7月20日，美國白宮首次發布聲明，指控中國資助黑客集團，對各國企業勒索數以百萬計美元；並且發動2021年3月對微軟電子郵件系統的大型網絡攻擊。該聲明提到，與中國國家安全部有關的黑客於2021年3月利用微軟交換伺服器 (Microsoft Exchange Server) 存在的保安漏洞，向全球數以萬計電腦系統發動網絡攻擊，導致不少公司機密數據外洩，並且蒙受巨額的金錢損失。美國，歐盟、英國、北約部分成員國，以及日本、澳大利亞、加拿大和新西蘭，接近40國譴責中國對全球網絡安全與資訊安全造成威脅。[16] 正是這事件導致美國總統拜登高調公開表示網絡攻擊可能是引致全球大國爆發熱戰的導火線。

看看另一個觸發神經緊張的例子，美國東岸最大燃油輸送公司Colonial Pipeline亦在今年5月9日遭到勒索軟件攻擊，該公司需要將部分電腦系統下線，輸油管及相關系統無法正常運作。由於Colonial Pipeline每日輸送的燃油佔美國東岸的45%，在輸送系統受到網絡攻擊後，全美國有18個州，包括佛羅里達、新澤西、紐約等的州政府，宣布進入緊急狀態，批准必要時可用陸路運輸方式運送燃油到各地。[17] 有消息指，黑客組織DarkSide是主腦，於5月6日入侵輸油公司管道的網絡，竊取接近100GB數據，並向Colonial Pipeline索取贖金；威脅若不照辦，被竊取的數據就會在網絡上公開。 這次網絡攻擊最令人擔憂的是，Colonial Pipeline是美國東岸重要的基礎建設

公司，被黑客攻擊系統後，需要緊急停止部分網絡連線，因而嚴重影響美國東部的燃油運輸。若然下次黑客的目標是機場系統、鐵路運輸系統或醫院電腦系統等基礎建設，會不會造成更嚴重的公共安全問題？相信公共設施或基礎建設的網絡安全，是目前多國政府最關注的事。

提到勒索軟件，一個頗矚目的例子是著名的日本遊戲公司Capcom於2020年11月因網絡攻擊，被黑客存取了公司部分郵件伺服器、檔案伺服器等系統，並造成部分公司網路無法運作。事後，勒索軟件Ragnar Locker的背後組織，聲稱是發動攻擊者，並已從Capcom在日本、美國及加拿大等公司的網路上竊取了1TB（等如1000GB）的資料，並且加密；威脅Capcom交付贖金。

從上述可見，個人、公司企業、國家基建，甚至國際關係，都要面對網絡不安全的威脅。在這個「萬物都能上網」，也就是「萬物」都可能受到網絡安全威脅的時代裡，到底一般人應該有什麼的資訊安全觀念，又應該要如何成為合格的「數位公民」，相信是很多讀者都會關心和留意的事。

保障個人資訊的可能：「不上網最安全」？

在探討個人資訊安全和網絡安全之先，必須先要處理一個很基本的概念——「不上網最安全」。除非擁有非常專業的知識和器材，甚至有自己的伺服器或相關設備，不然只有「不上網」才不會在網絡世界留下數碼足跡。但一般人很難做到不留痕跡，或是能夠「完全」刪去自己的數碼足跡。「不上網」顯然完全不符合現代人的生活習慣，就算是在很封閉的社會，還是會有少數人有機會使用互聯網及相關服務。所以「不上網」這做法，基本上只會在極端的情況下才會有人嘗試實踐。

既然是極端，為什麼要強調呢？因為部分對網絡安全一知半解的人存有不同的迷思。例如有人會覺得使用VPN或是能夠加密的通訊軟件，就能夠在網絡上「隱藏」，不會被人追蹤得逞。事實卻是，一般人非常難以「消滅」自己的數碼足跡，只有會「留下幾多」的差別。所以對資訊安全一知半解，反而是最危險。話雖如此，人類還是少不免需要網絡，因為互聯網真是很方便的工具，除了可以連接全世界，「萬物都能上網」基本上就是人類社會發展的趨勢。是故大家不如實事求是，採取認真積極的態度，去了解如何既使用網絡又能在最大程度上保障自己的資訊安全以及網絡安全。

筆者算是很在意一般資訊安全技巧的網絡使用者，但是在寫作這個課題之前，也報名參加了一個相關資訊安全的講座。從中聽到很多從來沒聽過，也沒有實踐過的的資訊安全知識和技巧，可見保障資訊安全的方法實在多得很。例如可以選擇使用管理密碼的軟件，又或是比Google雲端硬碟更為安全和保密的雲端服務。不過這些方法和實踐已是基礎以上水平的網絡安全知識；很多人可能連最基本的都還未清楚。所以接下來先介紹一些簡易可以做到，又有效保障自己的小知識和小技巧；若是覺得自己於網絡安全有更大風險的讀者，可能就要尋求更加專業的協助。

避開資訊安全陷阱

｜搜集資料｜

一個保障資訊安全的重要方法，就是不使用有資訊安全疑慮的軟件、網站和服務。疫情爆發之初，不少公司和政府剛開始容許職員「在家工作」的時候，就曾經有組織、學校、企業，甚至政府對部分通訊軟件的安全性感到疑慮。例如目前最多香港人習慣使用的ZOOM，曾經傳聞會將其收集到的通訊資料傳送至特定國家；因此有國家和公司在資訊安全考慮下，拒絕使用ZOOM作為通訊軟件，並要

求職員使用安全疑慮較低的通訊軟件。[18]

雖然要分析有資訊安全疑慮的軟件、硬件、網站或網絡服務，需要具備一定的電腦程式又或是網絡工程的相關知識，以拆解不同器材和軟件有沒有被加插不必要的程式碼，並推斷程式收集的資料會傳送到什麼地方。不具備專業知識的使用者，的確很難作專業的分析並破解。不過，每個網絡使用者，在使用任何電子產品、軟件或服務之前，仍然有能力作一定的資料搜集。例如購買電子產品，可以先了解產品的製造商，又或是先到軟件和網站服務供應商的網站，查看公司或軟件開發者的所在地。因為某部分國家和地區的電子產品生產公司、軟件開發公司和開發者，其資訊安全本來就令人疑慮；例如俄羅斯和中國的軟件公司便多次被指會將軟件收集到的資料傳送到特定的伺服器，或是放在程式；甚至有生產電子產品的公司被指會在其生產的硬體（例如手提電話或電腦處理器晶片等）附加用途不明的程式。「被加料」的電子產品除了會有更大的電力消耗，更可能早已植入監視軟件和程式，會在使用者不知情的情況下，收集其在現實及網絡上的活動資訊。不單威脅個人的資訊安全，甚至是威脅人身安全。[19] 因此，在選擇電子設備和使用軟件前，先作一些資料搜集，避免光顧有資訊安全風險的公司及其產品，很大程度上已經令個人資訊安全有了第一層保障。

如果對上述的資料搜集仍有疑問，不知道在什麼地方或網站才能查閱相關訊息，可以留意一些海外以報導電子產品和資訊科技業界消息為主的網站。[20] 那些網站不時會報導有關監視軟件、危險網站及軟件，甚至網絡世界有什麼嚴重的資訊安全意外和有什麼新型網絡攻擊正在發生。由於今時今日網絡安全與每個人的生活息息相關，所以當有嚴重的資訊安全危機出現，或有最新的安全資訊，很多中文傳媒都會翻譯和報導相關的消息。語言絕對不會阻隔資訊的流通，只要仔細留意便不難取得。

｜守護個人資料和密碼｜

同樣基本又不難做到，又能保障資訊安全的做法，就是不要隨便填寫和登記個人資料，亦不要輕易使用網頁瀏覽器的「保存密碼」功能。很多網站都會要求使用者先登記成為會員，才能使用相關服務，例如購物、訂座等。使用者應該在登記成為會員之前，留意該網站收集個人資料的細節；如非必要，千萬不要提供過多個人資料。若是在評估後認為該服務要求的個人資料不合理，就不要因為登記成為會員能方便使用相關服務或者得到好處（例如有贈品）而就範，以免得不償失。

同時要警惕的是，很多瀏覽器（不論電腦或是手提電話）都會提供「保存密碼」功能，方便使用者不需要每次登入網站，都要重新輸入密碼。不過，密碼保存功能其實也是隱形的資訊安全炸彈，因為黑客能透過入侵使用者的瀏覽器程式取得相關帳號的密碼，監視軟件。雖然不儲存密碼會造成不便，但不使用保存密碼功能，其實也是在最低程度能保障個人資訊安全的做法。

｜定期檢查並更新軟件｜

不論手提電話或是電腦，都需要時刻使用最新版本的軟件。因為每個軟件都不會是最完美的，總會有被破解的可能；定期按照程式開發公司要求，更新相關程式是其中一個保障資訊安全的重要步驟。Windows、Android、ISO等主要電腦和手提電話的作業系統，以及很多手提電話APPS開發商經常都會向使用者提供更新檔，要求大家下載並且更新。使用者絕對不能認為麻煩而不理會，因為更新作業系統和程式，很多時候是相關公司的程式員發現漏洞，在修復軟件和程式後提供的。

當然，電子產品作業系統更新經常會有「災情」，有時候世界

各地會傳出消息指，系統更新後反而會導致器材不能正常運作（甚至直接損壞）。所以毋須每次都要搶在第一時間更新電子產品系統，而是在服務供應商提供更新檔之後，先觀察一至兩日，甚至一星期才選擇更新程式，以避免裝置不能運作的風險。過新不好，但切記也不能讓相關的程式停留在過舊版本，因為過舊的程式和作業系統容易造成資訊安全風險。

提到過舊的硬件或軟件版本，可能有些讀者都曾耳聞APPLE、Google、Microsoft等作業系統公司，有時候會宣布將不再支援過舊的作業系統，例如Microsoft在2020年1月14日開始停止對Windows 7的支援，這代表程式開發商不會再更新相關的作業系統；即使有人找出新的程式漏洞，該公司也不會進行修復。是故，使用者應定期留意電腦和電話相關系統的更新。雖然舊器材仍能夠繼續使用，但要保障個人資訊安全，有時候的確只能「淘汰」過於陳舊的器材。

｜安裝合適的防毒軟件｜

安裝防毒軟件，並且定期更新，是保障資訊安全的重要方法。相信很多人早已在自己的電腦安裝防毒軟件，甚至連Windows系統也有為使用者預載了一些防護電腦病毒的功能，並鼓勵使用者安裝第三方的防毒軟件。不過，在選擇防毒軟件的時候，也需要先作資料搜集。有部分地區開發的防毒軟件，雖然是免費，但卻是眾所周知藏潛問題。已經知道的，有金山衛士、360安全衛士、百度殺毒等。曾經有人嘗試安裝多於一個的防毒軟件，卻發現電腦處理器在電腦沒有運作任何其他軟件的情況下，還是會處於100% 運轉狀態。而且瀏覽器首頁亦會被相關軟件「綁架」，強行設定為該軟件指定之網站，簡直比電腦病毒更像電腦病毒。[21] 當然，每部電腦理應只安裝一種防毒軟件，但中國軟件開發公司所開發的防毒軟件一向都存在無法刪除、綁架使用者瀏覽器首頁、賣廣告等問題；甚至在使用者沒有授權的情況下，將電腦數據上載到服務供應商指定的

伺服器，所以盡可能不要安裝相關軟件，以保障個人資訊安全。

只安裝一種防毒軟件，而且需要定期更新。因為黑客開發的病毒程式日新月異，若沒有定期更新防毒軟件的資料檔，令電腦防火牆知道要抵擋什麼病毒程式，那麼防毒軟件便發揮不到作用，安裝也是徒勞。所以在使用電腦時，可以定期開啟已安裝的防毒軟件，並且查看是否最新版本；若不是便馬上更新，也是有效確保電腦資訊安全的做法。

不過，電腦可以安裝防毒軟件防止病毒程式入侵，但電子產品例如智能電話，目前仍難以安裝非常有效的防毒軟件。[22] 筆者最近在一個資訊安全的講座上，仍然聽到講者提到礙於作業系統的問題，智能電話是至今仍然難以安裝有效防毒軟件的電子產品。所以保障智能電話的最佳方式，就是在兩大系統的Apps Store下載軟件，但要避免下載和安裝來歷不明的APK檔案，而且避免使用有問題的網站；不要隨便點開在社交媒體收到的連結網址，以及不要隨便使用不明來歷的無線網絡 (WIFI)。基本上，能堅持做到上述三點，智能電話的資訊安全就已經有了很大保障。

教會和教會機構的資訊安全

教會和教會機構，包括神學院，同樣要面對資訊安全的危機，筆者專程向一位宗派教會的牧者和一位神學院職員查詢教會／神學院處理資訊安全的做法。牧者的回應是其宗派沒有多大關注，宗派的總會沒有特別人手負責資訊科技，亦沒有特別的資訊安全指引。當然，這情況與該牧者所屬宗派總會與堂會的關係有關，因為該宗派在體制上不是事事都「由上而下」，堂會有非常大的自主性，所以總會不需要特別為堂會的資訊安全負責。另一個體制上相對比較「集權」的宗派，規定堂會需向總會取得網址，也需要將堂會的網頁存放在總會的伺服器內；所以這宗派的總會有專門的資訊科技部

門，以協助宗派整體的資訊科技事宜。遺憾是這部門的職員最終都沒有接受筆者的訪問邀請，所以無從得知該宗派目前所面對的資訊安全問題，以及教會有沒有特別因應近年資訊科技的發展而制定相關法規。

神學院處理資訊安全的做法又如何呢？筆者成功訪問了香港中文大學崇基學院神學院負責資訊科技及資訊安全的鄧長佑先生。他表示崇基學院神學院因為與香港中文大學關係密切，所以大部分資訊安全由大學資訊科技部門負責，壓力相對較小。他指出，香港有些神學院會因為各種原因會將在網絡公開的畢業學生名單作一定修改，有時又會刻意不公開來自某些地區的畢業生名字；原因是顧慮那些畢業生的人身安全。這種做法，其實就是本文論及資訊安全的時候，提及的「不上網最安全」法則。

筆者的另一個觀察，香港不少教會沒有如其他不同範疇的公司／機構般重視資訊安全，原因可能是教會通常沒有非常「數碼化」。以筆者所屬的宗派教會為例，教會很多重要資料，例如會友名冊、堂會及總會會議記錄等等，都沒有特別進行數碼化，亦沒有放到網絡上以供他人查閱（這可能會導致日後研究教會歷史方面的困難）。此外，如果不是有肺炎疫情，敝宗派教會的所有聚會根本不會在網絡進行，所有參加者都必須親身出席，那就沒有通訊軟件是否安全的問題。綜合上述兩種情況，敝宗派教會基本上沒有非常嚴重的資訊安全風險。唯一需要擔心的是，可能會有不法之徒製作假教會網頁，或是冒充教會職員向會友套取個人資料。不過以筆者所知，目前香港教會仍未出現相關案件。

不過，教會需要警惕的是閉路電視錄影片段，這可能是個資訊安全的缺口。閉路電視錄影其實不只在教會，所有公眾地方都有，甚至家庭以此來保障財物、家人或動物家人的安全。以前數碼攝影與網絡技術不發達的時候，由閉路電視鏡頭所拍攝的影像，解像度

不高，難以看清楚影像中的文字、樣貌和服飾；更不會存放在網絡雲端伺服器。 近幾年高清數碼拍攝和網絡技術的發展成熟，閉路電視所能拍攝到的影像已經清晰很多，甚至有資訊安全專家擔心，其清晰度已經可以看到影像手持的信用卡號碼。[23] 這種情況驅使筆者建議教會和教會機構應在合理的位置貼上提示，提醒路人該處有閉路電視攝影鏡頭。這樣，有資訊安全疑慮的人能夠作出適當反應，例如使用手提電話時要特別注意電話的畫面會否被拍攝。目前很多閉路電視鏡頭都能接上無線網絡操作，例如將拍攝到的影片自動上載到指定的雲端硬碟空間儲存，以方便使用者將影像下載，或是觀看；因此這些閉路電視通常會有原廠設定的器材名稱和無線網絡密碼。不過這些原廠的設定通常都是很簡單，而且密碼的安全程度不足。如果教會和機構選擇安裝相關的閉路電視器材，務必要將原廠的閉路電視密碼更改為具有一定安全程度的高強度密碼，以避免閉路電視鏡頭遭人入侵，盜取相關影像，造成資訊安全問題。同時，在購買閉路電視系統的時候，亦要留意生產商是否信譽良好。有些地區所生產的閉路電視系統，已經被多次指出有「後門」、設計上有缺陷，或是雲端硬碟伺服器的安全程度不足，容易被入侵或遭人惡意利用。所以教會和機構在購買和安裝閉路電視系統前，應要考慮安全性，不好只考慮價錢。

鄧長佑也提及幾個教會／教會機構目前可以考慮的資訊安全做法。首先，應事先評估正在進行或將會進行的事工是否存在資訊安全的風險，例如會否因資訊洩漏而對教會／教會機構整體造成不同程度的傷害，或是會令資訊被洩漏的人遭遇不同的風險。如果答案是肯定的話，教會／教會機構就有責任在事工開始前，決定要如何保留相關事工的資訊，甚至作出完全不保留資料的決定。第二，教會／教會機構必須考慮會友、使用者、職員等人的資訊安全。雖然資料數碼化是大勢所趨，同時在疫情期間，亦有愈來愈多會議改成在網上舉行；教會／教會機構亦會將崇拜錄影、日常報告及相關

資訊上載到網絡空間，以方便因疫情不能回到教會／教會機構的會友或使用者下載。不過，教會／機構都需要考慮相關的資訊安全，例如將資料加密、選擇存儲的載體，以及有權限下載那些資料的職員身分等。這些都是很多沒有留意資訊安全、沒有資訊安全習慣的教會／教會機構經常忽略的事宜。但在現今的世界中卻是愈來愈重要，甚至會因為忽略而造成嚴重的損失和傷害。

數位時代的數位素養

數碼與網絡世界「元宇宙」的說法，近日正引起廣泛討論，但香港基督教界也好，國際基督教界也好，都不多教會、基督徒和神學家在探討網絡世界與數位素養的問題。或者應該說，整體華人社會都不多討論。筆者在最近半年，才看到幾本與數位公民相關的翻譯書，令中文世界的讀者能夠了解相關議題。[24]

｜hacker / hacking｜

神學家Kate Ott是少數有出版學術專書討論數位時代的基督教倫理學學者，她的著作Christian Ethics For A Digital Society[25] 討論了數個與基督教倫理相關的數位社會問題，當中與本期主題比較相關的是第五章：。在英語世界裡，hacker 和 hacking 本來就有「非法」、「沒有取得他人同意的進入」等意思[26]，因此 Kate嘗試探討黑客及相關行為是道德與否，其實算是對既有常識或刻版印象的反省和思考。她認為黑客技術並沒有道德與否的問題，關乎道德的是如何應用資訊科技，和相關技術的人。[27] 一般人對黑客的印象（包括在使用中文的社會裡），都是「入侵他人電腦及系統，盜取資料或擾亂電腦系統的不法分子」，但現實中部分擁有黑客技術的人會利用他們的知識以協助不同公司改進其電腦系統；某些公司還會特別聘請他們做工程師，專門協助研發或搜索系統漏洞 。所以在當下世界，擁有黑客技術的人不一定就是在進行犯罪行為，又或hacking

也不一定就是犯罪；可以是改進電腦系統的手段。關鍵是技術的使用者如何運用已掌握的技術。

｜維繫網絡世界的多元性｜

Kate提出的另一個看法，看似是對基督徒，甚或是對所有會使用到網絡技術的人更重要的提醒；她在第一章提到關於「技術多樣性」的問題。她說很多神學家認為，聖經中的巴別塔故事並非很多基督徒一直以來認知的詮釋——上主因為人們以技術建築巴別塔來挑戰祂，因而打亂人類的語言；更有可能是上主不喜悅人們消除彼此的差異性，建立虛假的「統一」，因此才會在巴別塔的故事中，使人類重新出現差異，並且加以肯定。[28] Kate認為大家在使用網絡、社交網站等工具的時候，不容易意識到自己正被那些工具和技術「支配」，特別是搜索引擎、社交網站等有使用「演算法」的平台與工具。「演算法」(Algorithm) 簡單說來，是設計公式，之後將公式寫成程式，再讓電腦執行程式來計算答案。例如顧客在購物網希望在萬千貨品中盡快揀出心頭好，網站設定條件範疇讓顧客剔選以便盡快列出他們會考慮的貨品。然而演算法背後可以是隱藏了支配使用者的意圖，以及存在不公義的演算程式。例子是刻意引導使用者注意某些品牌、價格和產地，又或是具有種族歧視、歧視特定性別或性向群體。因此使用者須要留意並學習了解那些平台和工具的基礎功能，在了解平台和引擎後，才能關注、不被支配，甚至作出抵制。[29] 也許保持技術和網絡世界的多元性，才是上帝樂於見到的人類社會和技術發展方向。

也許對很多人而言（包括筆者在內），要學習程式設計、系統架構、網絡演算法等專業技術是很困難的事，而且一般人亦不太可能為了監察科技公司、社交網站或平台的運作，而特別學習非常多（甚至非常沒有興趣）與本科或本業無關的專業技術。不過作為消費者亦是使用者，理應也是技術或是產品的持份者之一。既然在實

體商品的世界裡，使用者也能透過消費來「投票」，選擇和淘汰自己想要和不想要的商品，那麼在網絡技術和資訊科技世界裡，使用者理應也能發揮同樣的角色，選擇和淘汰自己不想要的服務或服務供應商。

｜向霸權說不｜

要透過消費來選擇自己想要的未來並非容易的事，至少需要有一定數量的「已醒覺」消費者團結起來並成為一股力量，才有望向生產商或服務供應商成功施壓。相比實體商品，消費者在網絡世界和資訊科技世界裡，可能更難成為壓力團體；因為網絡平台要做到非常方便，才能吸引大批使用者選擇使用服務和購買商品。最大的例子是，現時家用電腦系統通用的就只有Apple的Mac OS與Microsoft的Windows30，使用者基本上沒辦法透過消費的方式來拒絕這兩家公司的營商手法或商品。不過，資訊科技世界的選擇不多，並非消費者毫無作為的理由。以Windows的發展為例，筆者印象中最能彰顯消費者力量的一次，應該算是Microsoft在2015年 推出Windows 10作業系統的時候。 Windows 7應該是最廣泛被使用和使用時間最長的作業系統，直到Microsoft在2012年推出Windows 8，並希望使用者自行將裝置更新為Windows 8。不過，Windows 8的開始鍵和相關選項的設計，令極多人不適應和給與劣評；以筆者所知，當年有非常多Windows使用者並沒有使用Microsoft提供的更新軟件，將電腦的作業系統更新為Windows 8，反而繼續使用Windows 7。一直到Microsoft於2015年推出Windows 10作業系統，將開始鍵的設計重新回到與Windows 7及之前十多年推出的Windows一樣，再加上宣布不再支援Windows 7；Windows 7的大部分使用者才選擇更新成Windows 10作業系統。

由Windows 7到Windows 10的發展過程，根本就是Windows的使用者用了消費者的力量，影響Microsoft將過於「新穎」的版面設

計改回到大眾習慣的模式的最好例子。它說明了即使是「大台」，只要消費者集體表達意見，甚至採取不更新的不合作行動來表達不滿，其實仍然有空間使服務供應商作出改變。

｜檢舉不法網站和服務｜

網絡世界和現實世界絕非兩個平行空間可以各自為政，實情是提供網絡世界的科技公司和服務供應者都要接受各地政府的規範。例如兒童色情相片和影片，於世界多國都屬違法，所以一般網絡供應商會很積極移除存在他們伺服器中的禁品。這些特殊的相片和影片，通常是有特殊困難／需要的人在自己架設的伺服器上擺放，為了逃避刑事責任會使用不同的技術來隱藏伺服器和使用者身分；各地執法人員要與不法之徒鬥智鬥力才能揪出背後的主謀。 可惜的是，能對應的法規沒有網絡及相關技術的發展來得快，無法規管日新月異的網絡世界。這種情況之下，作為消費者的我們，假如自認相對能跟上網絡世界的發展，而且知道其中的罪惡，好應該時刻保持敏銳觀察，檢視和反思各式服務。如果發現有不妥善的技術發展及可能用於不合法，甚至是存在不尊重人權、自由、民主的技術，就要向相關的體制反映，由政府以公權力作出規範。

這種希望規管網絡世界的說法，可能對於某些高舉互聯網世界有絕對自由的人來說，是不可接受的事。但近年不少社交平台上的亂象，例如之前解釋過的為了賺取更多金錢而以廣告誘導使用者購物的演算法，或可能背後隱含性別或種族歧視的演算法，都是社交平台網站或服務供應商沒有自律，為了賺取最大利潤而造成的惡果。如果使用者和現實世界擁有公權力的人，沒有意識和抗議高舉互聯網世界有絕對自由所造成的惡果，終有一天會被這種想法吞噬。然而，如何在規範與自由之間取得平衡，是一門藝術，也是值得人們警惕的事。某個國家最近就向世人展示了當公權力擁有過大的權力，可以在一夜間破壞網絡世界的所有可能；但是毫無規管的

網絡世界，同樣也會造成不可挽回的惡果。

在數位時代裡，如何讓公民成為更好的「數位公民」，擁有一定的數位素養，是很迫切的事。教會其實也可以思考在培養人們有更好，更適切的數位素養一事上，有沒有能夠扮演的角色。基督徒是否能夠在擁抱和尊重多元的同時，又能彰顯上主所創造的這個受造世界的美好——不論是在現實世界還是網絡世界。

注釋

1. 布魯斯．施奈爾著，但漢敏譯：《物聯網生存指南：5G世界的安全守則》（台灣：貓頭鷹出版，2020），頁20。
2. 行文至此，筆者不禁再次驚覺全世界「晶片荒」並非所謂的「飢餓行銷」，而真的是因為晶片需求實在太大，所以才會導致半導體生產成為了重要工業。
3. 廣義來說，智能器材就是指增添了電腦功能的器材，例如智能電話其實就是有電腦運算功能的手提電話，只是智能器材與以往人們習慣的「電腦」外觀不同，而且可以是任何想像到的器材。
4. 可能年輕的讀者，又或者家中在1990年代中期沒有電腦的讀者，並沒有經驗過56K電話線上網的時代，沒法理解上網就不能接通電話，接通電話就不能上網是一個怎樣的狀況。
5. 布魯斯．施奈爾著，但漢敏譯：《物聯網生存指南：5G世界的安全守則》，頁24。
6. 提到黑客，大家可能通常第一時間都會想到新聞提到部份公司被黑客入侵並且勒索，又或是想到一些電影中黑客入侵網絡的情節，那些行為固然是非法行為；但亦有些擁有黑客技術的資訊科技行業人士，會與不同的公司合作，以黑客技術尋找不同系統的漏洞，幫助那些公司改善自身系統，這些會「光明正大」入侵他人公司系統的黑客，的確是正當而合法地作出「攻擊」。
7. 〈拜登警告網絡攻擊可能導致與其他大國的“真正交火”〉：https://reurl.cc/3aVjx8，法國國際廣播電台（RFI），擷取日期：2021年8月12日。
8. 例如2021年4月便有新聞提到，香港婦人被假冒公安的騙徒多次合共詐騙2.5億港元，涉案金額相當驚人。〈假冒中國公安電話 香港90歲老太太被詐騙2.5億港幣〉：https://bit.ly/3Af3p3N，法國國際廣播電台，2021年4月20日，擷取日期：2021年8月12日。
9. 名為「hkjunkcall.com」的Facebook專頁於2021年8月15日所發佈之貼文：https://www.facebook.com/phoneadblacklist/photos/a.101045089018/10159434254784019/
10. 〈香港6間銀行涉違法洩露顧客個人資料〉：https://bit.ly/3nchr2B，法國國際廣播電台（RFI），發佈日期：2010年8月13日，擷取日期：2021年8月25日。
11. 不過其實若真的是個人資料被非法販賣，當事人其實也很難得悉自己的個人資料到底是被人從什麼途徑取得，但是這條例修訂對於部份曾經「光明正大」地販賣個人資料的公司，特別是銀行和保險行業而言，的確能起到部份阻嚇作用。

注釋

12.〈FB 5.33 億用戶資料疑遭洩漏　包括電話、名、電郵等〉：https://bit.ly/3l7cNAa，立場新聞，發佈日期：2021年4月4日，擷取日期：2021年9月5日。
13. 2020年初的時候，由於香港口罩供應緊張，所以部份公司在購入或生產口罩後，都以網絡派籌的方式分配購買口罩名額，有一部份網站在登記的時候，需要以個人全名、電話等個人資料以作核實之用，若那些公司並沒有做好網絡安全的話，收集到的資料可能也曾遭外洩而不知。
14. 可參閱報導"Video game maker EA says hackers stole source code"：https://techxplore.com/news/2021-06-video-game-maker-ea-hackers.html，Techxplore， 發佈日期：2021年6月10日，擷取日期：2021年9月5日。
15. "How Hackers Used Slack to Break into EA Games"：https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack，Vice，發佈日期：2021年6月11日，擷取日期：2021年9月5日。
16.〈【零日漏洞】五眼聯盟日本北約認定　黑客攻擊與中國國安有關〉：https://www.rfa.org/cantonese/news/world-response-07192021152033.html，自由亞洲電台，發佈日期：2021年7月19日，擷取日期：2021年9月5日。
17.〈美國最大燃油管道遭網絡攻擊 多州進入緊急狀態〉：https://www.bbc.com/zhongwen/trad/world-57054720，BBC中文網，2021年5月10日，擷取日期：2021年9月5日。
18. 例如台灣、德國、美國政府部份部門，還有部份跨國公司如Google、Tesla都拒絕使用Zoom作為通訊軟件，以免遭致資訊安全問題。可參閱報導"Who has banned Zoom? Google, NASA, and more"：https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/
19. 最新近的例子有立陶宛政府向其國民警示，指出中國公司生產的手提電話，會預先安裝不同的程式，部份具有審查功能。部份中國公司生產手機會在未經使用者同意的情況下，將手機數據傳送到他國特定的伺服器，而不知其用意，因此呼籲國民棄用中國公司所生產的手提電話。詳情可見報導〈立陶宛呼籲民眾棄用中國手機 小米華為回應〉：https://www.bbc.com/zhongwen/trad/world-58662398，BBC中文網，2021年9月23日，擷取日期：2021年9月25日。
20. 例如上述提及過的Techxplore便是其中一例，網址：https://techxplore.com/。
21. 可閱讀〈防毒軟體誰最流氓？陸網友養蠱式實測〉一文，網頁：https://www.

注釋

ettoday.net/dalemon/post/6796，Ettoday鍵盤大檸檬，日期：2015-01-07，擷取日期：10月2日。

22. 〈手機防毒 App 真的安全有用嗎？實測出爐：惡意程式偵測率最好的是這23款〉，自由時報：https://3c.ltn.com.tw/news/36163，日期：2019年3月15日，擷取時間：2021年10月2日。
23. 羅正漢：《生活資安五四三！：從生活周遭看風險與資訊安全》（新北市：博碩文化股份公司，2021），頁2-7至2-9。
24. 台灣出版社近年開始引入與翻譯數本新近而且和「數位公民」相關的著作，例如有主打童書和雜誌的親子天下翻譯和出版專為兒童而出版的童書系列《數位世界的孩子》（共四本），另外有八旗文化出版的《數字公民》和橡實文化出版的《數位公民素養課》，這些書籍出版的時間新近，相對具有參考價值。
25. Ott Kate, Christian Ethics for a Digital Society (Lanham: Rowman & Littlefield Publishers ,2018).
26. 例如在Cambridge Dictionary收錄的Hacker及hacking，均有提到黑客及黑客行為是"without permission"，甚至Hacker是"to do something illegal"，可參考網頁版Cambridge Dictionary：https://dictionary.cambridge.org/zht/%E8%A9%9E%E5%85%B8/%E8%8B%B1%E8%AA%9E/hacker及 https://dictionary.cambridge.org/zht/%E8%A9%9E%E5%85%B8/%E8%8B%B1%E8%AA%9E/Hacking
27. Ott Kate, Christian Ethics for a Digital Society ,131-135.
28. Ott Kate, Christian Ethics for a Digital Society ,20-24.
29. Ott Kate, Christian Ethics for a Digital Society ,36-38.
30. 還有Linux、UNIX等作業系統，但是這兩大系統不是太普及和商品化，通常是專業人士才會使用，家庭或個人用戶都是使用Mac OS及Windows為主。

《守望牧職》是新計劃「守望牧職」的其中一種實踐。在香港社會近年不同層面產生的變化中，學會除了實行自身既定的工作計劃，也思考如何支援教牧同工反思他們在社會的角色。就此，我們定下幾個目的：第一，為教牧同工提供對社會議題有厚度的認識，特別是神學和基督徒參與；第二，組織和推動教會與社區對話，甚至尋找合作可能，為建構社區的公民素質和健康的心理質素一同努力；第三，建議神學和信仰反省，豐富對牧職的想像。《守望牧職》正是以文字來實踐這三個目的。

學會每年財赤達五十萬，但沒有影響我們放慢使命。我們仍努力投入建立一個讓人有尊嚴的社會，並支援教會回應上主的使命。我們需要你們的同行。你們一句打氣的話、一點金錢的捐助是我們動力之一。

捐款方法：

- 劃線支票 — 抬頭「香港基督徒學會有限公司」或 Hong Kong Christian Institute Ltd.
  請將劃線支票連同姓名及聯絡方法寄往本會地址，或直接存入支票並通知本會。
- 銀行入賬 — 香港匯豐銀行，戶口號碼：196-035927-001。
  請將入數紙連同姓名及聯絡方法透過whatsapp (93520864)、電郵或傳真通知本會。

地址：香港九龍旺角塘尾道54-58號永利工業大廈 9/F 901室
電話：(852) 2398 1699｜傳真：(852) 2787 4765｜電郵：info@hkci.org.hk
凡捐款港幣100元或以上，可憑捐款收據申請減免稅款。


守望
牧
職