勿以電郵發送機密資料。 不要以電郵傳送個人資料，例如信用卡號碼、密碼、生日或社安卡號碼。每次要去公司網站時，最好重新登錄。大多數關注客戶資料安全的公司會讓登錄的客戶發送機密電郵到網站的客戶服務部，並且讓客戶通過公司網站接收回覆郵件。

檢查網站安全。 要先查證瀏覽器的網址欄為“https://”（而不是“http://”）。所有合法經營的金融機構及零售商網站均有使用SSL加密措施（安全接收資料層），因此可以確保客戶網上理財或付款的安全。

鎖上你所使用的無線網絡。 如果讓使用中的無線網絡保持開放狀態（unlocked），就有可能讓人在無線網絡通訊範圍內進入你使用的無線網絡而可能截取你所收發的資料。若要保障你的無線網絡的安全，可在你電腦的路由器（router）上設定密碼保護。

避免在公開的無綫網絡里購物或理財。如果必須要使用公開的無線網絡，要先確認你上的網站的安全性（https://），並要禁止他人分享你的個人資料，同時應採用個人專用虛擬網絡服務（VPN, virtual private network），例如Private WiFi（www.privatewifi.com），來保護你的網絡身份安全。

使用數據錢包。 你的銀行或付款公司可能會提供客戶數據錢包服務。當你在線上購物時不需要輸入信用卡號碼或其它的付款資料。所有開銷將由另外一個你預先註冊的帳戶支出，這樣可在你使用的網絡周圍加設安全屏障。

只和能夠信賴的個人或公司做交易。 在向一家沒有來往過的公司送出個人及付款資料以前，應先查核該公司信譽（消費者投訴及滿意程度）。只要在網上搜索一下該公司的名字，就可以獲得很多該公司資訊。

審查各種應用軟件（apps）。在下載任何一個自己並不熟悉的軟件以前，應該先查閱用戶評論及確認該軟件公司是否合法經營。用戶可以在“Settings”或“About This App”標籤下查閱有關軟件公司提供的用戶隱私權政策。TRUSTe公司授證予行動通訊應用軟件公司及各網站的隱私權政策，你可以先確認有無TRUSTe公司標記。如有必要，用戶可將應用軟件的隱私權保護範圍重新設定到令自己放心為止。請留意有些應用軟件需要先追蹤用戶所在位置才能有效提供服務。

警惕各類欺詐通訊。 如果你對某個電郵、短訊或電話的真實性有所懷疑，就不要回覆。你可以直接與該公司聯絡查明。因為合法經營的商業公司從來不會聯絡客戶索取社安卡號碼、用戶名、密碼或其它機密資料。如果你誤陷“引人上鉤”（phishing）的電郵圈套，並發現了自己的錯誤時，要立即更改帳戶密碼，以及通知開戶機構。用戶也可善用電郵網站所提供的垃圾電郵和引人上鉤電郵過濾網服務。平時瀏覽網站時，直接鍵入網址，而不要點擊電郵中的鏈接（link），因為你有可能會被誤導至冒牌網站。

小心防備惡意軟件（malware）。 用戶應使用對抗電腦病毒及反間諜軟件預先防備，並且要確保那些軟件均有定時更新，以便用戶上網時可以避免個人資料遭受惡意軟件竊取。你也可以啟動電腦內置的防火牆設備，在你的電腦及互聯網之間樹立一個虛擬屏障。

刪除舊的銀行及與轉帳相關的短訊。 如果在電話或其他通訊器材中有帳戶結餘或私人資料的舊短訊，應該將其刪除。

保護個人行動通訊器材。 由於智能手機和掌上電腦可以儲存大量機密資訊，卻又容易遺失或遭竊，用戶應多費工夫設定保護措施。你可以設定密碼鎖住暫時不用的手機，或是當手機閒置了幾分鐘後就會被鎖住。

清除電腦器材內部硬件。 當你在出售、捐贈或棄置自己的電腦及行動通訊器材時，要先清除硬盤上的資料，這項功夫會比刪除一般的檔案複雜。查詢刪除方法，可以點擊求助欄“Help”，或是相關廠商網站，也可以用手機或掌上電腦與自己的無線通訊公司聯絡。 ReCellular (www.recellular.com/recycling/data_eraser/default.asp)專門提供清除各種類型手機的說明指南。如果你的電腦或手機是由僱主提供，可聯絡公司負責管理的員工協助處理。而身為員工要注意僱主有權利獲取公司擁有電腦器材上所儲存的所有資料。

協助與諮詢

Federal Trade Commission www.ftc.gov

聯邦交易委員會（FTC）教育社會大眾在商業世界中如何保護自己，在與商家交易時如果有消費者權益及隱私權相關爭議，可向FTC提出投訴。

消費者行動

Consumer Action

www.consumer-action.org

消費者行動之諮詢熱線向消費者提供建議及轉介服務：

電郵：hotline@consumer-action.org，或致電：415-777-9635

有中文、英文、西班牙文諮詢專員覆電。

Digital Dollar系列刊物由消費者行動製作出版，Visa Inc.贊助發行。

VISA

consumer action
Education and advocacy since 1971

可以上網瀏覽Visa金融教育計畫－Practical Money Skills，網址：www.practicalmoneyskills.com

查詢有關如何保護帳戶資料的要訣及實際應用操作，避免付帳卡詐騙，以及解決金融卡未經授權而遭盜用的問題，請瀏覽相關網頁：www.visasecuritysense.com,可選英文或西班牙文。

Your Digital Dollars - Mobile Safety and Privacy（Chinese Version）

數據金融理財

用互聯網及行動電話金融轉帳的安全及隱私提要

以數據通訊處理銀行事務及付款時應如何保護個人身份及資料不遭盜用

這本金融理財社區教育手冊是由消費者行動及Visa Inc. 共同提供

當今人們的生活日漸繁忙，不論是購物、理財、工作或社交，都需依賴電腦或行動通訊器材，因此造成個人資料曝光的機會大增。

目前雖然已有很多安全措施加強了網上轉帳的安全性，但是有些使用網絡或行動電話的消費者仍然要面對個人隱私被侵犯的風險。個人資訊可能在未得到你的同意時經由幾個方式洩露，例如使用公用的無線網絡通訊、遺失智能手機，或是意外顯示了個人密碼。所幸如今也有很多方法及工具能夠保障你在網上或在外出途中使用網上轉帳的安全。

為何安全使用互聯網或行動電話理財是十分重要？

雖然互聯網及行動通訊科技的各項功能改善了人們的生活，但同時也會產生許多問題而導致消費者的個人資料被竊取、無意洩露或遭誤用。例如一個身份盜用者可以在全世界任何角落以詐騙不實的網站引誘你洩露網上密碼。用戶的智能手機也可能儲存很多密碼及帳戶資料，一旦遺失，也許比丟了錢包還危險。而且如果某個你去過的網站將你的資料交給其他人，那麼你會常收到（可能還很煩人的）垃圾廣告電郵（spam），甚至一些未經你授權的帳目開銷。

如果你能提高警惕，同時常常留意相關資訊，還是可以避免上述情形的發生及其它的潛在困難。

使用互聯網或手機理財的消費者所面臨的各項風險

郵件遭到攔截或機密談話被竊聽，是一些人人都可能遇到的風險。而在網上及使用行動通訊器材理財或付帳，你的隱私也會有被侵犯的風險。

你的電腦或手機遺失或遭竊後，他人可能會取得你的私人資料、帳號以及付款記錄。

有人可以半路攔截你使用無線網絡發送或接收的信息。

騙子可以引誘你將個人資料輸入一個假冒的仿造網站（copycat），或是回覆一封詐騙電郵（phishing）。

數據曝光（一個金融機構的數據存庫遭竊或在無意間洩露了資料），可以造成你或其他消費者的身份資料落入盜用者之手。

有些你所熟識的人可能會猜測到或無意發現你的帳戶密碼。或是你因為在公用電腦以及沒有設定保護措施的行動通訊器材儲存了用戶名及密碼而泄露密碼，這等於給了入侵者一把開門鑰匙。

你的電腦或行動通訊器材可以經由間諜軟件或其它具有破壞性的軟件（malware）而感染病毒，個人資料因而被盜取。

有些公司可能會將收集來的個人資訊轉售出去，或讓其它公司用來做市場推銷或其它用途。有些個案就是因為公司之間分享客戶付帳卡資料而造成一些未經持卡人授權的錯誤開銷。

挑選公司及產品應注意事項

如果想保護個人資料，最好的辦法就是只跟那些致力於保障消費者及網頁瀏覽者的安全和隱私的金融機構、商店、應用軟件以及其他公司做交易。當你考慮選擇公司、產品或服務時，請注意以下幾點：

合法性： 一個設計出色的網站並不等於它是合法經營或可以信賴的。如果你不太熟知該公司的信譽，應先上網查一下它是否屬實、客戶的滿意度，以及公司投訴記錄等等。也應該查證其它相關資訊及消費者索賠記錄（例如可以撥打其網站所列出的電話號碼）。

加密措施： 在瀏覽器旁邊有一把扣上的鎖或是沒有破損的鑰匙，同時網址上的“http”字體後面附有“s”（“https://”），可以顯示出該網站是有安全保障及加密措施的。（也就是說相關資訊是用密碼傳送出去，只有指定的收件人才能認讀）。一個網站上如果有VeriSign或McAfee的公司標誌，就表示他們有加密服務或其它相關科技以保障客戶的資料安全，你可以點擊那些標誌查核有關該網站的相關資訊。

額外的安全功能： 如果用戶的網上帳戶在登錄後的一段時間內靜止不動，網站會自動將其帳戶退出，這是額外安全保障的例子。因為你離開電腦卻未退出帳戶或關閉瀏覽視窗，網站自動將你的帳戶退出可以防止他人介入你的帳戶。另外一個好現象就是在你登錄網站時需要接受雙重“認證”，例如是一張你選用的圖片以及你對它所做的描述，同時外加用戶名稱及密碼。

“零責任”政策： 這可以保證你不需擔負因未經授權的交易所造成的損失，而且帳戶里被竊取的金錢損失將會得到補償。

強而有力的隱私權保護政策： 相關政策應該很清楚地公佈在公司的網站上，詳列公司如何收集、使用以及儲存消費者的個人資訊。理論上來說，公司應該說明他們不會將客戶的資訊和第三者（毫無關聯的個人或組織）分享。如有必要，你應該很容易要求 “退出”（opt out），不得將個人資訊和他人分享 。網站上若有TRUSTe或BBBOnline組織標誌，就表示該網站可以信賴或是有強力的隱私權保障。（你可以點擊那些標誌來確認該網站是否合法—其網址應該和公司被授證的網址相同）。如果你對於該網站的隱私權保護政策不滿意，可立即退出。

有時候公司收集消費者的資訊也未必不好。很多有信譽的公司或商家就憑那些資訊來改善服務及效率，令客戶使用網上或行動器材來理財的經驗更加愉快及有效率。但是有些公司利用消費者的資訊去做積極的市場促銷，出售客戶資訊給一家或多家第三方買主，或沒有盡力預防駭客劫取資料，防止不良的公司職員或他人不當使用客戶資訊。所以當你考慮光顧哪家公司，和提供多少個人資料給這家公司時，你要警覺小心謹慎做此決定。

保護個人隱私要點

只透露必須要登記的資料。 當你註冊網上服務或開立帳戶時，只填寫表格上必須填寫的部份。（那些空格前面通常會列出星型符號）。如果可以選擇，最好選擇填盡量少透露自己的資料。若是為了得到免費試用品或優惠券而填寫資料，你所填報的資料就有可能會被出售或公開做市場促銷及推廣。

善用瀏覽器內的功能。 目前比較新型的互聯網瀏覽器有預設保護個人隱私的功能在內。所以當你即將被誤導至一個詐騙網站時，瀏覽器會發出警示來保護用戶。如需查詢相關資訊，可以詳讀瀏覽器上的協助欄（Help section），同時應該定期更新你的瀏覽器軟件，以便更好地利用它所提供的最新隱私保護功能。

掌控個人電腦中的網站瀏覽記錄檔案（cookies）。 Cookies 是一些網站儲存在你電腦中的小檔案，用來追蹤記錄你瀏覽過的網站活動資料。而記錄資料的主要目的是用來做市場促銷，但也可以用來記錄客戶的網購訂單以及是否該網站的老顧客。你可以設定在退出網站時，瀏覽器立即自動刪除cookies的記錄功能，或者完全不接受cookies的記錄功能。也可以考慮根據不同的網站啟動或停止cookies做記錄。如需查詢相關詳情，可至瀏覽器協助欄（Help section）。

保護個人密碼。 要為你的電腦、行動通訊器材、金融帳戶，以及各種應用軟件設定強而有力的密碼，而且不要向任何人透露。千萬不要將密碼儲存在有你的金融資料或私人資料的網站里—包括那些存有客戶信用卡檔案的零售商。你可以考慮在每次購物時才輸入付帳卡號，而不要讓商家將帳號存檔，因為這樣具有風險性。

退出網站（log out）。 當你登錄某個金融網站，付費網站或手機應用軟件進行理財時，千萬不要離開你的電腦或是行動通訊器材。如果線上操作已告一段落或暫時需要離開螢屏時，應隨時退出網站並關閉應用軟件或瀏覽視窗。如果是公用電腦，可在大多數的網頁上點擊“Tools”標誌，然後選擇“Delete Browsing History”或是“Clear Private Data”，這樣可以清除你瀏覽過的網站記錄。