1– 常見欺詐行爲

http://www.infosec.gov.hk/tc_chi/promotion/security_animations.html

互聯網爲我們帶來不少資訊及服務。有些電子服務需要確認使用者身分，例如涉及：

※ 金錢交易的服務，如電子銀行服務；
※ 收費的服務，如訂閱收費雜誌；
※ 登記的服務，如網上查閱個人資料；
※ 法律責任或合約條款的服務。

但稍一不慎，便會蒙受欺詐，招致損失。

常見欺詐行爲四部曲：騙徒會

1. 盜取你的個人資料作憑證 (credentials)；
2. 冒認你的身分登入認證系統 (authentication system)；
3. 利用你的身分進行交易、享用服務或作電子簽署；
4. 令你蒙受不同程度的直接或間接損失。

盜取憑證和冒認身分

騙徒會利用不同的手法盜取憑證，如透過：

※ 欺詐網站；
※ 欺詐電郵；
※ 欺詐電話；
※ 欺詐信件。

騙徒會建立一個虛假網站，使用幾可亂真的虛假網址或網頁(如以www.ebank.org假冒www.bank.org)，誘騙你進入網站並提供個人資料。誘騙手法包括：

※ 發出緊急或提示電郵，要求你點擊超連結(hyperlinks)以確認帳戶資料；
※ 發出抽獎或中獎的彈出式視窗 (pop-up window)、電話或信件，要求你提供個人資料以領取獎賞；
※ 在討論區、電郵等附設超連結，讓你一不留神便進入欺詐網站。

騙徒會根據服務及認證系統的不同需要，盜取你的個人資料以冒充你的身分，例如：

※ 用戶名稱；
※ 密碼；
※ 身份證號碼（全部或部分）；
※ 信用卡號碼；
※ 信用卡到期日。

進行交易以圖利

騙徒會利用你的帳戶及身分進行交易，例如：

※ 銀行轉帳或交費；

※ 網上購物；
※ 訂購服務；
※ 查閱你的戶口資料，如交易記錄；
※ 提交附有電子簽署的文件；
※ 以你的帳戶名義接受條款。
這些交易會令你蒙受不同程度的直接或間接損失，例如：金錢損失、資料泄漏、責任承擔。

提示
爲免受欺詐，我們要時刻提高警覺。以下有幾點建議：
※ 將重要或常用網站加入書籤，以確保進入正確網址；
※ 避免點擊不熟悉的超連結，並小心核實所連結到的網站；
※ 除非已確認對方身分，否則避免向任何人或經電子渠道披露個人憑證和敏感的個人資料；
※ 留意有關欺詐的消息和個案，如金融管理局發放有關虛假網址的消息，了解欺詐手法。

總結：提高警覺 免受欺詐

2－ 核實身分

對很多人來說，電子交易甚爲方便快捷。爲確保交易可靠及值得信賴，資訊系統會在交易前進行認證程序，以便：
※ 使用者以電子形式向資訊系統確立其身分以建立信心；
※ 確定憑證在有關交易中是否有效；以及
※ 確定憑證並無逾期、被撤銷或撤回。

視乎潛在風險和所須達到的信任程度，資訊系統會核實以下資料以確定使用者的身分：
1. 使用者所知的資料(如密碼)；
2. 使用者擁有的憑證(如身份證或權標)；以及/或
3. 使用者的特徵或行爲的資料(如指模或話音識別)。

認證系統一般涉及兩個主要程序：註冊和認證。註冊程序包括兩部分 ： 註冊和撤銷。
1 註冊
   i. 註冊－可以是一次過的程序，完成後便能享用網上服務；
   ii. 撤銷－不再需要某項網上服務時須進行的程序。
2 認證－每次交易都須進行的程序。

註冊
視乎潛在風險和所須達到的信任程度，服務提供者會規定使用者以不同方式註冊，例如：
1 使用者親身遞交身分證明文件以供核實身分；
2 使用者遞交書面申請，並在申請表上簽署作實或夾附身分證明文件；或
3 使用者以電子方式註冊和提交其個人資料(如電郵地址或手機號碼)。

使用者或須在閱讀及接受某些使用條款後才可完成註冊程序。

成功註冊後，服務提供者會就有關服務爲使用者開立帳戶或讓使用者透過其現有的帳戶註冊。服務提供者也可提供憑證予使用者，讓使用者於其後交易中作認證之用。有關憑證包括：
※ 帳戶名稱及初始密碼（或個人識別號碼）；或
※ 保安權標－ 所顯示的號碼會作爲密碼的一部分。

註冊提示
※ 你可以只提供必需的資料作註冊用途；
※ 如不想提供某些個人資料或接受某些使用條款，你可以放棄註冊；
※ 你應盡快更改初始密碼或個人識別號碼；
※ 你應妥善保管密碼、個人識別號碼或權標，以免被他人盜用。

認證
爲了核實使用者身分，提供有關服務的資訊系統會在進行電子交易前，要求使用者提供帳戶名稱及一項或多項憑證，例如：
※ 密碼或個人識別號碼；
※ 保安權標所顯示的限用一次密碼；以及/或
※ 數碼證書。
如交易需要較嚴格的認證，通常會採用多重認證。認證因素越多，便越能確定使用者的身分。使用者可以考慮有關交易的認證項目是否足以核實身分，他們亦須慎防憑證使用不當可能涉及的風險。

認證提示
※ 進行交易前須確定網站的真確性；
※ 進行交易後須記錄交易資料，如記下交易參考編號及日期等或保存有關交易記錄列印本；
※ 完成交易後須完全登出資訊系統；
※ 定期更改密碼或個人識別號碼；
※ 妥善保管個人識別號碼或保安裝置；
※ 定期查閱帳戶交易摘要及登入記錄。

撤銷
在以下情況，你或須暫停或撤銷已註冊的服務：
※ 懷疑帳戶被盜用；
※ 遺失權標。拾獲者可能會用該權標冒認你的身分；
※ 不再使用該項服務。

撤銷提示
爲盡量減少你須承擔的責任或所蒙受的損失，我們建議：

※ 如不再使用有關服務，應盡快要求服務提供者撤銷帳戶；
※ 遇上以下情況，應盡快通知服務提供者：
  ※ 身分資料有變，如接收限用一次密碼短訊的手機號碼；
  ※ 遺失保安權標；或
  ※ 發現不尋常的交易或活動記錄。

一般提示
爲確保電子交易穩妥可靠，電子服務應採納一重或多重認證以核實使用者的身分。在整個認證過程中，使用者應：
※ 在註冊使用電子服務時，小心謹慎提供個人或敏感資料及接受使用條款；
※ 妥善保管憑證(例如密碼或保安權標)，慎防被他人盜用以冒認使用者的身分；
※ 在進行電子交易時，確定有關網址屬真確無誤才登入，並在完成交易後登出；
※ 記緊撤銷閒置帳戶，以免被人擅用。

總結：核實身分 安心交易

3－ 常見威脅(盜用身分)

我們廣泛使用電子身分進行電子交易。雖然使用電子身分有助建立信任及確保交易穩妥可靠，但由於騙徒會利用電子認證程序的漏洞騙取使用者資料，故不當使用電子身分會爲使用者帶來更大威脅。

註冊
騙徒可能會利用你的個人資料，以冒充你的身分辦理註冊。可從以下情況取得你的個人資料：
※ 你在不經意的情況下在欺詐網站註冊，並提供不必要的個人資料；
※ 你曾向他人或機構披露個人資料，而對方未經你的許可不適當地使用這些資料。

如你收到電郵、短訊或信件指你已註冊或曾使用某項服務，但事實並非如此，則你的身分可能已被盜用。要糾正這情況，你須：
※ 立即通知服務提供者有關不尋常情況，並撤銷有關帳戶；
※ 檢查有關服務是在什麼情況下註冊，以及曾進行哪些交易；
※ 檢查你所蒙受的損失和須承擔的責任，並與服務提供者商議責任誰屬；
※ 如有需要，報警求助。

認證
騙徒可利用你的帳戶及憑證，以你的名義進行電子交易。他們可以從多個途徑取得你的憑證：
※ 偷看：騙徒可能從你背後偷看，並抄下你的帳戶名稱及密碼；
※ 猜測密碼：騙徒可能利用一些可猜測密碼的工具或技術，試圖猜出你的密碼；
※ 透過終端機取得資料：騙徒可能透過你剛使用但忘記妥善登出的終端機取得你的資料；
※ 欺詐網站：騙徒可能透過欺詐網站盜取你提供的帳戶和憑證資料；或

※ 遺失權標：騙徒可能拾獲你遺失的權標或手機，並因此取得你的限用一次密碼。

如發現一些不屬於你的交易記錄或登入活動，你可能已被他人盜用身分。你必須：
※ 立即通知服務提供者有關不尋常情況，並撤銷有關帳戶；
※ 檢查曾進行哪些交易；
※ 檢查你所蒙受的損失和須承擔的責任，並與服務提供者商議責任誰屬；
※ 如有需要，報警求助；
※ 如有需要，開立另一個帳戶或更改密碼。

提示
要保護你的電子身分，你應：
※ 妥善保護你的個人資料，切勿隨便向他人披露。
※ 切勿在公共終端機(例如咖啡店或圖書館的終端機)或不安全的終端機，進行認證或登入使用已註冊的電子服務；
※ 確保使用後登出資訊系統；
※ 選用一個易記難猜的密碼；
※ 檢查網站的真確性，切勿在來歷不明的網站提供敏感資料或帳戶資料。

總結：保障身分 免被盜用

4－ 上網時的良好習慣

現時幾乎任何地方，如家居、公眾場所、或使用流動裝置均可上網。在以下例子，阿政展示了一些上網時的良好習慣。

1. 使用安全終端機
阿政在咖啡店內想使用電子銀行轉帳。不過，爲安全起見，他決定回家使用自己的個人電腦，而不使用店內提供的公共終端機。
提示：切勿經由公共或不安全的終端機登入使用該類電子服務或進行認證。

2. 傳送資料要加密
阿政在家使用自己的電腦，每次在使用電子銀行服務傳送敏感資料前，都會檢查瀏覽器與網站之間的連結是否已加密。
提示：應以加密格式傳送敏感資料(如：密碼)。

3. 檢查網站真確性
登入網站前，他亦會檢查網站的保密插口層證書，以確保網站的真確性。
提示：應檢查網站的真確性。

4. 使用強密碼

他會使用至少由8個數字、字母和標點符號混合組成的密碼登入網站。
提示：應選用易記難猜的密碼。

5. 定期檢查帳戶
登入後，他會檢查帳戶狀態、活動及登入記錄，以偵測可疑的地方。
提示：應定期檢查帳戶狀態、活動及登入記錄。

6. 勿點擊可疑網站連結
當使用網上服務時，一個即時信息視窗彈出，並提供一個網頁超連結。對於這類來歷不明的信息，阿政概不理會。
提示：切勿點擊來歷可疑的網站連結。

7. 使用後登出
使用電子銀行轉帳後，他會完全登出系統，以免帳戶被他人盜用。
提示：應於使用後登出網站。

總結：認證有法 安全上網

5－ 離線時的良好習慣

阿政除了展示上網時的良好習慣外，他亦向朋友阿玲展示了如何在離線時保護帳戶憑證。
1. 留意最新消息
阿政介紹阿玲觀看一則有關僞冒網站的新聞。該網站看似用作進行抽獎活動，但真正目的是套取個人敏感資料作欺詐用途。
提示：應留意有關僞冒或可疑網站的最新消息。

2. 密碼與帳戶資料分開放
阿玲從錢包取出載有用戶名稱及密碼的字條，以便按字條上的用戶名稱及密碼登入使用電子銀行服務。阿政告訴他不應這樣做，正確的做法是牢記着一個易記難猜的密碼。
提示：切勿將密碼與帳戶資料放在一起。

3. 妥善保管保安裝置
在完成交易時，電子銀行要求阿玲提供一個限用一次的密碼。不過，她的硬體權標卻遺留在辦公桌上。阿政提醒她要好好保管保安裝置，勿讓他人取得。
提示：應妥善保管認證卡及保安裝置，一旦遺失或被竊，應立即註銷。

4. 常備緊急電話號碼名單
阿政跟着向阿玲展示一張緊急報失電話號碼名單。如遺失密碼或權標，或發現任何不尋常的帳戶活動，應立即通知相關機構。
提示：應備存所有帳戶的緊急或報失電話號碼名單。

5. 切勿共用帳戶
因沒有權標，阿玲想借用阿政的帳戶進行交易，但遭阿政拒絕。
提示：切勿與他人共用帳戶/密碼。

總結：憑證資料 妥善保管

6－ 選擇密碼

密碼是使用者與服務提供者之間的秘密。容易破解的簡單密碼，即使沒有外泄，亦可能會給別人猜中。爲加強保護以免歹徒有機可乘，應使用難以破解的密碼。

一般原則
阿政告訴阿玲應如何選擇密碼。密碼應：
※ 包含大小寫不一的英文字母；
※ 包含數字，甚至標點符號；
※ 可供快速輸入。
提示:密碼應以最少8個大小寫不一的英文字母、數字和標點符號混合組成,並可供快速輸入。

阿玲問阿政會否用他那頭小狗的名字作密碼。阿政表示不會。
提示：切勿以自己、家人或寵物的名字作爲密碼。

除了名字，不應使用他人容易取得的資料作爲密碼，例如：生日、周年紀念日或電話號碼等。
提示：切勿使用他人容易取得的個人資料作爲密碼。

阿玲表示同意，並補充說詞典所載的詞彙亦不宜用作密碼。
提示：切勿使用英語或外語詞典、拼字表或其他詞彙表/縮寫表中的詞彙作爲密碼。

以順序按鍵方式設定的密碼容易被人猜中，而使用者在輸入密碼時也容易被人偷看。
提示：切勿以順序按鍵方式設定密碼。

阿玲表示，有些網上服務提供有關帳戶和密碼的示例給使用者參考，只作示範，不應使用。
提示：切勿使用示例作爲密碼。

總結：使用易記難猜的密碼
選用難以破解的密碼，既可保護個人憑證，亦可讓我們享用安全的網上服務。

7－ 推行電子認證系統(1)

互聯網現已成爲業務發展不可或缺的一部分，提供了平台讓企業以較低成本迅速處理交易事

項。爲取得實質業務利潤，必須確保所進行的電子交易穩妥可靠，不得讓騙徒有機可乘。中小企東主阿翰想透過網上購物擴展業務。他從事資訊科技工作的朋友阿森建議他推行電子認證系統，確保真正的顧客可取得其業務資訊。

有系統的程序

電子認證系統可因所採用的技術、相關的管理措施，以及推行和營運成本而各有差異。阿森建議阿翰依循以下程序推行電子認證系統。有關程序包括以下五個主要步驟：

1. 評估風險
2. 釐訂保證等級
3. 釐訂要求
4. 實施保護措施
5. 監察、報告和審核

評估風險

就電子認證系統而言，最主要的考慮因素是估計涉及的風險，以及這些風險對業務的影響。承受風險的能力越薄弱，則受到的影響便越嚴重，因此有需要推行認證較嚴謹的系統。

首先，阿森講解五類常見風險和四種不同程度的潛在影響，供阿翰參考：

五類風險

※ 不便、憂慮、地位或名譽受損
※ 金錢損失或法律責任
※ 未經授權發放個人和商業資料
※ 任何人士的人身安全
※ 違反民事或刑事法規

各類風險之下四種不同程度的潛在影響

※ 沒有影響– 沒有可量度的影響
※ 低度影響– 有限度和短期影響
※ 中度影響– 嚴重的短期影響，或有限度的長期影響
※ 高度影響– 極爲嚴重、災難性或嚴重的長期影響

釐訂保證等級

阿森建議阿翰參考「電子認證」網站(見本短片結尾時所示網址)載列的評估參照表，以便因應經確定的風險和影響爲其業務釐訂保證等級。

總結：評估風險 釐訂等級

企業須推行電子認證系統，以確保電子商貿穩妥可靠地進行。在上述建議程序中，首兩個步驟可助企業東主爲特定業務釐訂所需的保證等級，而接着播放的短片「推行電子認證系統(2)」所載述的其餘步驟，則可助他們定出用戶註冊和認證規定、研究可實施的保護措施，以及進

行監察和審核。

8－ 推行電子認證系統(2)

阿森是中小企東主阿翰的朋友。阿森已向阿翰介紹了推行電子認證系統的首兩個步驟。阿翰現已知道其業務的保證等級。阿森繼續向阿翰講述餘下步驟。

釐訂要求
可根據所釐訂的保證等級，對聲稱的身分定出信心程度，以及制訂實際的註冊和認證程序。阿森講述每個保證等級的要求，並就每個保證等級舉例說明可使用的認證技術。

第1等級
註冊方面並無特定的核實身分要求。可使用簡單的密碼作認證，確保使用服務者是註冊用戶。

第2等級
註冊方面有一定基本要求，以核實使用者的身分。可在加密網絡連接對話中使用管理密碼權標，以確保憑證或身分權標確實由註冊用戶控制。

第3等級
註冊方面有嚴格要求，以核實使用者的身分。可使用數碼證書作認證，以確保認證權標確實由註冊用戶控制。應採取措施，防禦竊聽、中繼攻擊和密碼猜測，以及防止有人冒充檢查員。

第4等級
此「保證等級」的要求與第3 等級相若，惟有關用戶必須親身辦理註冊，並以硬件權標作認證。可使用硬件權標內置的數碼證書，以進行遠程雙重認證。

在各種認證技術中，數碼證書是獨一無二的，可符合電子交易較嚴格的保安規定，所以阿森建議使用數碼證書作註冊及認證。

實施保護措施
除了因應保證等級採用適當技術和進行認證程序外，還須採取一些相關的措施，例如安裝防電腦病毒軟件和防火牆、爲用戶提供培訓及公布實務守則等，以加強系統的整體保安。

監察、報告及審核
阿森提醒阿翰即使系統推出後，仍須持續進行監察、審核及評估，以確保電子認證系統穩妥可靠，並能配合先進科技進步和應付環境轉變(如攻擊技術)。

總結：釐訂要求 實施保護
企業須推行電子認證系統，並應採用數碼證書，以確保電子商貿可以穩妥可靠地進行。上述所建議採用包含五個步驟的程序，可有助企業東主推行本身的電子認證系統。

9－ 釐訂保證等級

中小企東主阿翰希望擴展其保健產品業務，使其產品可透過網上訂購。他一名從事資訊科技工作的朋友阿森建議他在有關業務系統採用電子認證，並簡介了推行電子認證系統的五個步驟。阿森與阿翰一起檢視了一些業務功能，並協助阿翰釐訂適用的保證等級。

電子通訊

阿森指出，第三者可能在未獲授權的情況下取得某用戶所登記的用戶編號，但有關用戶因此而感到的憂慮、蒙受的損害或招致金錢的損失一般只屬微乎其微，甚至是量度不到。

對於電子通訊服務，第1 保證等級已屬足夠。用戶只須提供電郵地址便可享用這項訂閱服務。

網上訂購

阿森表示，雖然騙徒可能會假裝透過網上訂購產品及得知交易情況，但招致金錢損失的風險並不高，因爲有關交易及付款安排最終必須由有關用戶親自處理。此外，交易完成或被拒後，即使訂單狀況資料外泄，也只會造成短暫影響，有關用戶的其他敏感資料仍得到安全保管。

在評估風險後，建議釐訂爲第2 保證等級。客戶在網上註冊時須提供身分資料(例如全名、電話號碼及現時地址等)以供核實之用。如要訂購產品，客戶在登入認證程序時或須輸入用戶名稱及使用管理密碼權標。

網上查詢病歷資料

阿翰的公司備存了會員的病歷資料(如食物或藥物過敏)以便爲會員建議適用的產品。阿森認爲這類病歷資料一旦被他人取閱，長遠只洩露了有關會員的個人私隱，影響有限；但公司的聲譽則會於短期內嚴重受損。

可考慮釐訂爲第3 保證等級。客戶須親身前往阿翰的店舖完成註冊程序，並提供身分資料，例如全名、出生日期、電話號碼及現時地址等，以供核實及記錄。阿森並建議使用數碼證書，以便客戶日後登入系統及查閱病歷資料時核實其身分。

網上更新敏感個人資料

阿翰的公司備存了會員資料庫，載有一些熟客的個人資料及醫療記錄等。未經授權披露該等敏感個人資料，可引致嚴重或極爲嚴重的長遠影響，甚或須承擔法律責任。

對於涉及敏感個人資料的系統，建議釐訂爲第4 保證等級。阿森提醒阿翰必須嚴格核實用戶身分，例如規定用戶須親身辦理註冊申請，而登入系統時須證明持有硬體權標，例如智能卡內置的數碼證書。

總結：簡單工具 釐訂等級

保證等級可顯示註冊及認證程序中的信心程度。

以下網站載有互動工具，可協功釐訂適用的保證等級：
http://www.e-authentication.gov.hk/tc/business/assurancelevel.htm

10－ 雙重認證

阿祖需要在某個資訊系統推行電子認證模組。他的同事阿倫介紹了三個基本認證要素：
※ "使用者所知的資料"；
※ "使用者擁有的憑證"；以及
※ "使用者的特徵或行爲的資料"。

認證要素和認證方法
阿倫就每個認證要素講述一些常用的方法：

"使用者所知的資料"：
1) 以密碼及個人辨認號碼認證– 密碼或個人辨認號碼只有使用者才知道。

"使用者擁有的憑證"：
1) 公開密碼匙認證 – 私人密碼匙由使用者保管。
2) 對稱密碼匙認證– 限用一次密碼的權標由使用者擁有。
3) 以短訊服務認證– 手機由使用者持有。

"使用者的特徵或行爲的資料"：
1) 生物識別 – 指紋、瞳孔或視網膜等均是獨一無二的個人特徵。

雙重認證
要採用較嚴格的認證方法以核實登入者的身分，阿倫建議採用雙重認證要素以核實使用者的身分。由於雙重認證採用多一個認證要素核實身分，故一般比單重認證穩妥可靠。
進行高風險的網上銀行交易便是一個實例。使用者應持有儲存於智能卡(例如香港智能身份證)或電子鑰匙(例如USB 認證鑰匙)的數碼證書及私人密碼匙，並知道正確密碼，才能確保穩妥地進行高風險的網上交易。

總結：加強認證 多重保護
在電子認證過程中，採用的認證要素越多，所建立的信心便會越大。

11－ 常用的認證方法

阿祖剛從阿倫得知，推行電子認證系統涉及三種認證要素和五種常用的認證方法。
阿祖希望多些了解每種認證方法的實例。阿倫於是更詳細向他講解該五種常用的認證方法：
※ 以密碼及個人辨認號碼認證
※ 以短訊服務認證

※ 對稱密碼匙認證
※ 公開密碼匙認證
※ 生物識別

以密碼及個人辨認號碼認證
操作原理：使用密碼或個人辨認號碼登入是最常用(基於所知)的認證方法。
實例：使用密碼登入香港公共圖書館系統預訂借閱圖書。

以短訊服務認證
操作原理：短訊服務可傳送由資訊系統所發出的限用一次密碼。使用者透過手機所示訊息收到密碼後，可輸入該密碼完成認證程序。
實例：登入網上銀行系統時以短訊服務認證。

對稱密碼匙認證
操作原理：就對稱密碼匙認證而言，使用者與認證系統伺服器共用一條獨一無二的密碼匙。認證系統可向使用者提出「質疑」，要求對方向系統的伺服器發出經私人密碼匙加密的隨機訊息作爲認證。系統伺服器會利用共用密碼匙與收到的加密訊息「應答」進行配對，如吻合的話，便可證明使用者的身分。該認證方法的一個變更方案，是使用限用一次密碼權標，爲使用者產生限用一次密碼，以跟由伺服器產生的限用一次密碼互相配對核實。
實例：使用限用一次密碼登入網上銀行系統。

公開密碼匙認證
操作原理：公開密碼匙加密技術提供了可使用配對密碼匙(私人密碼匙與公開密碼匙)的認證方法。私人密碼匙由使用者私下保管，而相配對的公開密碼匙則通常內置在核證機關所簽發的電子證書。有關的電子證書可供其他人使用。
實例：向選舉事務處更新登記選民的住址資料。

生物識別
操作原理：生物識別方法是把個人的生理或行爲特徵以數碼方式轉爲認證資料(編碼值)，透過比較有關生物特徵的編碼值與儲存值，以核實使用者所聲稱的身分。
實例：香港入境事務處的「旅客e-道」採用指紋認證。

總結：認證多法 選擇使用

現有不同的認證方法、解決方案及推行方法，可配合業務所需的保證等級、使用者的需要及經費預算。選用一種或多種認證方法，以增強對交易的信心。

各種常用認證方法的比較載於以下連結：
http://www.e-authentication.gov.hk/tc/professional/compare.htm

12－ 其他考慮因素

阿倫已向同事阿祖介紹了五種常用的認證方法和雙重認證。他現在講述可在推行電子認證系統時採取的其他紓緩措施。

五項其他紓緩措施

1. 用戶端的控制 :End-user control

※ 可採取措施以便在某程度上取得用戶端的控制或保持連貫性，包括：
  ※ 使用特製的硬件設備；或
  ※ 於用戶端安裝簡化認證技術的解決方案軟件，無須依賴用戶按照正確程序操作。

※ 這項措施需要用戶合作才可推行，以保護他們免受各種型式的惡意攻擊。

2. 帶外管理的考慮因素：Out of band considerations

※ 「帶外管理」解決方案可應用於高風險交易，或作爲純技術解決方案以外的選擇。「帶外管理」通常涉及用戶與服務供應商之間一些並非單透過互聯網進行的通訊或資料傳輸。

※ 「帶外管理」的例子包括手機、短訊服務、電話通訊或傳統郵件。

※ 推行時會因使用帶外設備而引致額外費用。

3. 程式編製技巧：Programming Techniques

※ 黑客可利用合法網站作爲背景，然後把虛假網站疊放在上面。一些程式編製語言(例如 JavaScript)能偵測網站的部分是否嵌入框內，並能將這網站的合法部分(合法網頁)移往前面。這可防止上述欺詐技倆得逞。

4. 處理登入失敗的情況：Handling of unsuccessful login attempts

※ 妥善處理登入失敗的情況，可有助減低密碼猜測攻擊的風險。一些常用的處理方法包括：當登入失敗的情況超過了預定次數後，有關帳戶或接達權限便會暫停，或強制用戶等候一段較長時間才可重新嘗試登入。

※ 這種處理方法可納入密碼政策，即是說，除了設定密碼期限和要求密碼必須符合最低強度外，也可一併採用這種處理方法。

5. 交易記錄和帳戶活動監察：Transaction records and Account activity monitoring

※ 應定期向用戶提供詳細的交易記錄，以便他們識別欺詐活動。此外，亦應定期檢查帳戶活動，以查出不尋常之處，因爲這些不尋常之處可能是欺詐活動。

※ 系統應設有讓用戶檢查和報告事故的功能。

提示

阿倫建議阿祖應在系統推行初期考慮採取部分上述措施，例如：

※ 在設計階段，應在有關規格註明是否把用戶端控制、帶外裝置和活動監測納入系統設計。

※ 在程式開發階段，可推行和測試能防禦一般黑客技術的程式編製技術，並採用這種程式編製技術構建系統。

總結：紓緩措施 加強保護

鑑於科技進步，未來推出的嶄新認證技術和相關解決方案，將更爲先進精良、成本更低，而且更方便易用。我們應留意電子認證的最新消息，以加強這方面的保護。

13－ 電腦病毒及電腦蠕蟲

電腦病毒(Computer Virus)是一種最常見的惡性程式碼(Malicious Code)，會附在其他檔案或程式上，並會在程式執行時自我繁殖，對電腦造成損害。

電腦蠕蟲(Computer Worm)是另一種經常遇到的惡性程式碼。它跟電腦病毒不同，是一種會自我複製的電腦程式，不需附在其他程式或檔案上，能透過系統連結來傳播，消耗受影響電腦的資源或導致其他損害。

電腦蠕蟲可以在用戶不容易察覺的情況下，透過不同方法自動傳播到其他電腦或流動裝置(例如手提電話、PDA 等)。傳播媒介包括電郵、即時訊息(Instant Messaging)、多媒體短訊(MMS)、藍芽(Bluetooth)檔案等。

由於電腦病毒和電腦蠕蟲的感染徵兆及預防措施相似，以下會以電腦病毒作爲例子說明。

感染途徑
你的電腦在甚麼情況下可能會受到電腦病毒的感染？
※ 安裝或開啓來自不可信任來源的檔案或濫發電郵上的附件；
※ 造訪惡意的網站，例如虛假網站等。

電腦受病毒感染的徵兆
如果你的電腦受到電腦病毒的感染，會有以下徵兆：
※ 不能啓動防毒軟件或不能更新防毒軟件的最新病毒識別碼；
※ 電腦的效能降低；
※ 可供使用的系統記憶體或磁碟容量銳減；
※ 電腦出現來歷不明或新建立的檔案或程式；
※ 電腦出現異常重啓或死機。

防範措施
日常使用電腦時應該：
※ 安裝防毒軟件(Anti-virus Software)或包含防毒功能的反惡性程式碼軟件(Anti-malicious Code Software)，使用最新的病毒識別碼(Virus Signature)或惡性程式碼定義檔，啓動即時偵測功能及每週最少全面掃描電腦一次。
※ 安裝並啓動個人防火牆。

※ 安裝最新保安修補程式。
※ 無論是惡性程式碼定義檔或是保安修補程式，相關軟件的「自動更新」功能都應經常處於啓動狀態。
※ 定期爲程式與資料備份。
※ 在使用便攜式電子裝置前，預先對該裝置進行電腦病毒掃描。

只靠技術措施保護你的電腦並不足夠，切記：
※ 不應瀏覽可疑或不可信賴的網站或從中下載軟件；
※ 不應安裝來歷不明的軟件；
※ 不應開啓來歷不明的電郵和即時訊息或其附件等。

考考你
1. 電腦病毒和電腦蠕蟲是否都是常見的惡性程式碼？

2. 以下哪一個是有效預防電腦病毒的方法？
A) 開啓來自不明來源的電子郵件
B) 安裝防毒軟件及啓動即時偵測功能
C) 安裝來歷不明的軟件

14－ 濫發電郵 I

濫發訊息(Spam)一般是指在不管收件人同意與否，或在收件人已要求發件者停止送訊息的情況下，使用公共網絡發出大量訊息。訊息形式可包括電郵、傳真、電話短訊或多媒體訊息等。由於濫發訊息涵蓋範圍廣泛，我們只會特別介紹與電腦最相關的「濫發電郵」。

「濫發電郵」是指發出大量電郵推銷產品和服務，或散播惡性程式碼(Malicious Code)如電腦病毒。濫發電郵者期望有收件人會回覆電郵，對電郵內介紹的產品或訊息感興趣。

如何辨別濫發電郵？
如果電郵符合下列一個或多個條件，就很可能是濫發電郵：
※ 電郵沒有清楚及準確地列出發件人或機構的真確資料。
※ 商業電郵的標題不明確或有誤導性。
※ 電郵沒有「取消接收的選項」或「取消接收選項的陳述」。
※ 內容與許多收到的電郵相同或相似。

濫發電郵者如何收集電郵地址？
很多機構把他們的電郵地址在網上公佈，讓濫發電郵者很容易取得相關資料，並納入其濫發電郵名單中。這些機構，極容易遭濫發電郵的襲擊。

濫發電郵者一般透過專門幫助濫發電郵的軟件，藉掃描網上留言區及新聞組張貼的訊息、盜

取電郵地址名單及搜尋網站所載的電郵地址，建立目標名單。

潛在威脅
大量的濫發電郵不但對收件人造成煩擾，還會增加網絡負荷，浪費網絡的帶寬(Bandwidth)，虛耗大量磁碟容量，使收件人需花費金錢和時間去處理。

濫發電郵也是傳播惡性程式碼或電腦病毒的溫床。若濫發電郵帶有已受惡性程式碼或電腦病毒感染的附件，收件人開啓該電郵或附件後，電腦便會受感染。收件人的電郵帳戶可能會被控制。惡性程式碼會以收件人的名義，向通訊錄中的電郵地址，發出帶有已受電腦病毒感染附件的濫發電郵，傳播電腦病毒。

考考你
1. 「濫發電郵」一般是否指不管收件人同意與否，發出大量電郵到大量的電郵地址？

2. 以下哪項是一般濫發電郵的目的？
I) 散播惡性程式碼
II) 推廣產品或服務
III)測試網絡的負荷量
A) I & II
B) I & III
C) II & III

15－ 濫發電郵 II

如何處理濫發電郵？
遇上來歷不明或可疑的電郵，切勿開啓或隨便回覆，應把它們刪除。如果你回覆這些電郵，你就會同時向寄件人證實你的電郵地址是一個有效的地址，結果可能收到更多濫發電郵。

檢查電郵戶口的寄件匣，留意是否有並非你發出的電郵。如有，你的電郵戶口可能已被濫發電郵者控制用來發送電郵。你應立即中斷網絡連線，並立即啓動防毒軟件，掃描你的電腦，以及重設電郵戶口密碼。

如果你的電郵戶口已嚴重充斥濫發電郵訊息，請考慮停用你目前電郵戶口，並轉用一個新設立的電郵戶口。

如有需要，你可考慮向你的互聯網服務供應商查詢或求助，並夾附濫發電郵的標題資料。視乎個別供應商的政策，濫發電郵者可能會被警告、暫停以致終止服務。

防範措施
防範措施包括保護電郵地址及個人資料，和保護你的電腦。

※ 在網上提供個人資料時(如申請免費電郵帳戶時)，要小心謹慎，仔細查閱網站或公司私隱政策聲明以及服務的使用條款。
※ 不要在公開網站、聯絡人目錄、會員目錄或聊天室披露你的電郵地址。
※ 盡量使用不同的電郵地址作不同用途。例如：使用兩個不同的電郵地址作聊天室和個人通訊用途。
※ 避免使用字典裡簡單的字和通用的姓名作爲電郵地址。濫發電郵者可以採用自動化軟件，串連一些字典內常用的詞彙、名稱、字母和數字，組成電郵地址來濫發電郵。
※ 安裝過濾電郵軟件，自動過濾及刪除濫發電郵，減少接收的數量。雖然你不能以過濾電郵軟件阻止別人向你濫發電郵，但卻可阻止那些電郵在你的收件匣出現。
※ 過濾電郵方法有很多種，一般都可根據寄件人的電郵地址、域名或電郵的標題、內容等來過濾電郵。例如，用戶可設定或使用一些黑名單(Blacklist)(即拒絕接收電郵的地址名單)來過濾電郵。
※ 你必須在電腦上採取基本保安措施，安裝反惡性程式碼軟件如防毒軟件，並安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，及啓動相關軟件「自動更新」功能。

考考你

1. 最簡單處理濫發電郵的方法，是否不開啓該電郵，並且將它刪除？

2. 以下哪一個措施能預防電郵地址被濫發電郵者採集 ？

A) 不要在公開網站披露你的電郵地址。
B) 瀏覽可疑網站。
C) 回覆來歷不明或可疑電郵。

16－ 間諜軟件及廣告軟件

「間諜軟件」(Spyware) 是惡性程式碼的一種。當電腦安裝上間諜軟件，在用戶不知情下，間諜軟件會將用戶電腦內的檔案、用戶網上活動的資料，甚至用戶敲鍵的內容，秘密轉送。

「廣告軟件」 (Adware or Advertising-supported Software)是指附帶廣告的軟件。在程式執行時，它會自動下載一些廣告，並在螢幕上自動顯示及播放。某些廣告軟件同時也是間諜軟件，會附上間諜程式。

感染途徑

你的電腦在甚麼情況下有可能會被安裝上間諜軟件或廣告軟件？

※ 從可疑的來源，如網站、對等式 (Peer-to-peer，P2P) 網絡等下載或安裝軟件。這些軟件可能已隱藏了間諜軟件或廣告軟件。
※ 部分廣告軟件甚至不通知使用者，秘密地自動安裝。

感染的徵兆

如果你的電腦安裝了廣告軟件，電腦可能會出現以下未獲得你的同意的改變：

※ 瀏覽器的「首頁」變爲另一個網站，以一般設定瀏覽器的做法，你是無法更改這個首頁的。
※ 「我的最愛」資料夾中加入新的連結項目。
※ 新的軟件組件如瀏覽器工具列等會加在瀏覽器上。
※ 即使當你的瀏覽器並未開啓或者系統沒有連結到互聯網，帶有廣告的彈出視窗仍會出現。

潛在威脅

如果你的電腦安裝了間諜軟件或廣告軟件，你會面對怎樣的資訊保安威脅？
※ 安裝廣告軟件後，螢幕上自動顯示的廣告，可能會令你感到煩擾。
※ 一般間諜軟件能竊取及蒐集電腦及個人資料，如電郵地址、姓名及信用卡號碼等，然後將蒐集到的資料秘密轉送至別人。這些資料可能會被轉賣作市場推廣或其他不法用途。
※ 如果入侵者從蒐集資料中，發現你的電腦內有保安漏洞，可能會藉此植入惡性程式碼 (Malicious Code) 如特洛依木馬(Trojan Horse)，以入侵或控制電腦作不法用途。

防範措施

要防止受到間諜軟件或廣告軟件的威脅，你應該做好防範措施，包括：
※ 不要從可疑來源如網站、對等式網絡等下載或安裝軟件。
※ 在下載與安裝合法軟件前，要先閱讀使用條款與條件，因爲他們可能會要求你接受安裝某些搜集資料的程式。
※ 當造訪某些要求安裝外掛程式 (Plug-In) 或允許主動式內容 (Active Content)在電腦上執行的網站時，必須仔細閱讀使用條款。
※ 刪除瀏覽器內的瀏覽歷程記錄。

另外，你必須爲電腦採取基本保安措施，包括：
※ 安裝反惡性程式碼軟件如反間諜軟件，使用最新的惡性程式碼定義檔，啓動即時偵測功能及每週最少全面掃描電腦一次。
※ 安裝和啓動個人防火牆軟件。
※ 安裝最新保安修補程式。
※ 無論是惡性程式碼定義檔或是保安修補程式，相關軟件的「自動更新」功能都應經常處於啓動狀態。

考考你

1. 廣告軟件是否一種在執行程式時在螢幕上顯示廣告的軟件？

2. 以下哪一個是間諜軟件的定義？

A) 假裝提供正常功能，實際上帶有惡意破壞功能的軟件
B) 利用電子郵件引誘網絡用戶透露私人資料
C) 在未經用戶允許的情況下，將用戶電腦及網上活動的資料秘密地轉送至別人的軟件

17－ 仿冒詐騙

仿冒詐騙(Phishing)，又名網絡釣魚，是一種網絡詐騙形式。犯罪者利用仿冒電子郵件或欺詐網站，誤導毫無戒心的網絡用戶，輸入個人資料。

仿冒詐騙電郵

「仿冒詐騙電郵」，通常會涉及大量散播附有回郵地址、連結和品牌標記的欺詐性「僞冒」電郵，令電郵看似來自銀行、保險代理、零售商或信用卡公司。這類欺詐電郵的目的，是誘騙收件人相信電郵內容，跟從電郵內指示，登入仿冒詐騙網站，提供帳戶名稱、密碼、信用卡號碼及身份證號碼等個人資料，然後使用這些資料作其他非法活動。

仿冒詐騙網站

「仿冒詐騙網站」，即是使用與合法網站相似的域名(Domain Name)或子域名(Sub-domain Name)、或複製合法網站的外表及真確內容，如圖像、文字或公司標記，以誘騙訪客輸入帳戶或財務資料。

仿冒詐騙電郵所設的連結，會誘導收件人連接到欺詐網站，而非網頁上所顯示的合法網站。

潛在威脅

如果你受到仿冒詐騙攻擊，你將會面對甚麼威脅？

由於這些電郵幾可亂真，有些收件人會作出回應，登入仿冒詐騙網站，結果是個人資料外泄、財務上受損失、身分被盜用/利用作其他欺詐活動。

防範措施

要防止被仿冒詐騙，我們在使用電腦時要注意什麼地方？

※ 開啓電郵附件時要提高警覺，也不要按電郵內的連結進入網站。

※ 不要登入可疑網站，或連接這類網站內的連結 。

※ 不要從搜尋器的結果連接到銀行或其他金融機構的網址，應以人手直接輸入URL 網址或進入之前已加入書簽的連結。

※ 進行網上銀行交易時，可使用雙重認證(2-factor Authentication)，例如密碼加智能卡，來核實用戶身分。

※ 在完成網上交易後，切記要打印、備存交易記錄或確認通知，以供日後查核。

※ 提供個人或帳戶資料時，應保持警惕。銀行及金融機構絕少透過電郵要求客戶提供個人或帳戶資料。如有疑問，應向相關機構查詢。

※ 定期登入網上戶口，檢查帳戶狀況及上次登入日期，確定是否有可疑活動。

※ 收到信用卡或銀行結單後，應立即檢查是否有未經授權的交易或繳費。

※你必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，及啓動相關軟件「自動更新」功能。

考考你

1. 仿冒詐騙是否指利用假冒電子郵件或欺詐網站進行詐騙？

2. 以下哪一個是有效預防仿冒詐騙的方法？
A) 在網吧的公用電腦進行網上銀行的交易
B) 隨意打開副檔名是 "pif"，"exe"，"bat"，"vbs" 的電郵附件
C) 不要按電郵內的連結進入網站，而以人手輸入URL 網址

18－ 社交工程攻擊

從資訊保安的角度，社交工程攻擊是指利用人性弱點或哄騙他人提供個人或敏感資料，例如銀行帳號、私人密碼等，危及電腦系統安全。

社交工程攻擊例子
以下是一些典型的社交工程攻擊例子:
※ 攻擊者致電機構內部電腦支援中心的員工，自稱是機構的某高級職員，要求對方重設該高級職員的密碼，並將新密碼給予攻擊者。攻擊者取得新密碼後，便可假冒該高級職員，登入機構的電腦系統作進一步攻擊。
※ 另外，大意的員工往往會把一些載有敏感資料的文件或儲存媒體等棄置於垃圾箱內，使攻擊者有機可乘，輕易地從垃圾箱內找到有用的資料，進一步攻擊機構的內部電腦網絡。
※ 有些攻擊者則向受害者發送虛假的電子郵件，如果受害者對郵件深信不疑，便會依從指示進入虛假網站，並輸入敏感資料。這樣，攻擊者便可輕易取得這些資料，作非法用途。
※ 除此以外，攻擊者會用最簡單的偷窺方法盜取資料，例如當用戶輸入密碼時，在其身旁偷看，如果用戶一不留神，密碼便會泄漏。
※ 攻擊者也會利用一般人選擇密碼的傾向及慣性，猜測用戶密碼。用戶名稱、住址、出生日期等資料都不宜用作密碼，因爲容易被猜中。

保安措施
要減低社交工程攻擊的風險，可採取以下的保安措施：
※ 不要隨便把個人或敏感資料交給陌生人或不可信的機構。
※ 不要按下可疑電郵內的網頁連結。
※ 在未曾核實網站的可信性和安全性前，千萬不要傳送個人或敏感資料至該網站。
※ 使用較強的密碼，例如"1+Tw0Eq3"，並定期更改。
※ 在電腦螢幕上安裝有防偷窺功能的保護片，以防止攻擊者在旁窺看螢幕顯示的敏感資料。
※ 最重要是提高個人對資訊保安的知識，加強防範意識。

考考你
1. 下列哪項是一般的社交工程攻擊手法？
A) 在垃圾箱內尋找有用的資料
B) 趁用戶輸入密碼時在其身旁偷看
C) 根據一般人選擇密碼的傾向及慣性，猜測用戶的密碼
D) 以上皆是

2. 下列哪項不是針對社交工程攻擊的保安措施？
A) 不要按下可疑電郵內的網頁連結
B) 隨便把個人或敏感資料交給陌生人
C) 在電腦螢幕上安裝具有防偷窺功能的保護片
D) 使用較強密碼，並定期更改

19－ 中間人攻擊

中間人攻擊(Man-in-the-Middle Attack)，一般是指攻擊者在訊息傳送時，於發送者和接收者之間，暗中讀取、插入及更改訊息的網上攻擊。

入侵途徑
如果發送者在傳送訊息時，沒有將訊息加密(Encryption)，又沒有數碼簽署(Digital Signature)，攻擊者便可利用網絡上的保安漏洞，中途攔截及改變發送者的訊息，再傳回接收者。由於網絡傳輸仍能正常運作，沒有斷線，發送者和接收者都難以察覺傳送的數據，已被攻擊者竊取、攔截或竄改。這種攻擊，一般毋需在用戶電腦上裝上惡性程式碼(Malicious Code)，如電腦病毒或特洛依木馬(Trojan Horse)，也不會在用戶電腦上留下任何紀錄，因此難以被反惡性程式碼軟件(Anti-Malicious Code Software)如防毒軟件發現。

潛在威脅
受到中間人攻擊，你會面對甚麼潛在威脅？
若電腦用戶進行沒有加密的網上交易，中間人便可從傳送的訊息中讀取用戶的銀行帳號及密碼，登入帳戶，偷取金錢，或進行非法交易，令用戶蒙受財務損失。
如入侵者能竊取機構系統登入帳戶及密碼，便有機會盜取機構內部的敏感資料，如客戶個人資料，引致資料外泄。

一般保安預防措施
爲了有效防範中間人攻擊，你必須做好保安預防措施。

機構方面：
※ 採用加密連線，例如 HTTPS、SSH、SFTP 等等，把網絡的傳輸內容加密。即使入侵者可中途攔截，也不能閱讀或變更資料。
※ 使用相互認證(Mutual authentication)，由於用戶的電腦必須通過伺服器(Server)認證，而伺服器亦要通過用戶認證，因此可助阻隔中間人攻擊。

個人方面：
※ 設定和啓動 Wi-Fi 通訊的加密功能，如 WPA 以 AES 加密。
※ 在使用網吧或其他公共上網設施時，不要進行網上交易活動，或使用網上銀行。

除將訊息加密、使用數碼簽署及採取上述的保安預防措施外，其他各種相關的資訊保安措施，都不可以忽視。

考考你

1. 一般的中間人攻擊會不會在用戶電腦上留下任何紀錄？

2. 哪項保安措施有助預防中間人的攻擊？

I) 啓動Wi-Fi 通訊加密功能

II) 使用相互認證

III)在公眾地方用網上銀行

A) I & II

B) I & III

C) II & III

20— 竊聽

竊聽(Eavesdropping)是指在未經授權的情況下，擅自監察別人的通訊內容。

竊聽可以在一般電話系統、電子郵件、即時通訊系統或其他互聯網服務中進行。由於竊聽過程沒有阻礙網絡傳輸的正常運作，發送者和接收者都難以察覺傳送的數據被竊、截取或竄改。

隨着互聯網的普及，我們互相通訊時可利用各種方便的網上服務，如電郵、聊天室、社交網站等。如果我們使用這些通訊途徑時沒有採取適當的保安措施，被竊聽的潛在風險便會增加。

竊聽的方法

竊聽行爲通常會透過以下方法進行:

※ 以電郵爲例，如果發送者在傳送訊息時，沒有將訊息加密(Encryption)，又沒有數碼簽署(Digital Signature)，攻擊者便可利用網絡上的保安漏洞，作出中間人攻擊(Man-in-the-Middle Attack)，中途攔截及竄改發送者的訊息，再傳給接收者，使接收者誤信已被竄改的訊息內容，因而被騙取個人或敏感資料。

※ 一般互聯網都經由超文字傳輸規約(Hypertext Transfer Protocol，HTTP)標準傳輸數據，利用HTTP 標準傳輸個人或敏感資料是有欠安全的方法，因爲這方法不會把電腦用戶進行的網上交易加密，攻擊者可從傳送的訊息中讀取敏感資料。

保安措施

要減低在互聯網通訊時被竊聽的風險，可採取以下的保安措施：

※ 採用加密連線，例如 HTTPS(Hypertext Transfer Protocol Secure)及SSH(Secure Shell)等比較安全的方法，把在互聯網上傳輸的內容加密。即使攻擊者可中途攔截，也不能輕易地讀取或竄改資料。

※ 在連接互聯網的電腦上安裝個人防火牆，並配備安裝了最新病毒識別碼或惡性程式碼定義

的防毒軟件。

※ 使用公共上網設施時，盡量不要進行網上交易活動或使用網上銀行服務。

※ 應在機構的電腦網絡上安裝網絡入侵防禦系統(Intrusion Prevention System)，偵測及預防竊聽者的進一步攻擊。

※ 使用設有相互認證(Mutual Authentication)的互聯網服務，例如公開密碼匙基礎建設(Public Key Infrastructure，PKI)。用戶電腦必須通過機構的伺服器認證，而機構的伺服器亦須要通過用戶電腦的認證，待雙方身分確認後才進行網上交易，這樣受到中間人攻擊的機會便會減少。

考考你

1. 竊聽行爲可以在下列哪項系統進行？

A) 電話系統

B) 電子郵件系統

C) 即時通訊系統

D) 以上皆是

2. 下列哪項是針對竊聽行爲採取的保安措施？

A) 採用加密連線，例如 HTTPS 及SSH 等，把在互聯網上傳輸的內容加密

B) 使用公共上網設施時，盡量不要進行網上交易活動

C) 使用設有相互認證的互聯網服務

D) 以上皆是

21－ 鍵盤側錄程式

鍵盤側錄程式(Keylogger)是一個裝置或程式，用作擷取在鍵盤上輸入的數據。

入侵者能利用鍵盤側錄程式，一般以遠端遙控的方式記錄及監察使用者的所有鍵盤輸入，擷取輸入電腦的個人資料，如信用卡號碼、用戶帳號及密碼。因此，鍵盤側錄程式也屬於惡性程式碼(Malicious Code)的一種，與間諜軟件相似，它的目的都是偷取資料。攻擊者在進行攻擊時，可能將鍵盤側錄程式混合其他惡性程式碼一起使用。

入侵途徑

鍵盤側錄程式入侵電腦的途徑與電腦病毒相似，你若有以下行爲，攻擊者便有機可乘。

※ 安裝或開啓來歷不明的檔案或軟件；

※ 開啓來歷不明的電郵及其附件；

※ 造訪惡意的網站如虛假網站。

潛在威脅

入侵者可透過收集到的資料來監察用戶的所有鍵盤活動，尋找有價值的資料，尤其是帳戶號碼及密碼。然後，假扮用戶盜用其身分作非法用途。例如：

※ 登入用戶網上銀行帳戶，更改其戶口的登入密碼，偷取戶口金錢，或利用戶進行非法交易。

※ 登入用戶電郵信箱，更改其戶口登入密碼，再利用電郵戶口來濫發電郵及散播電腦病毒。
※ 登入用戶曾進入的系統，偷取系統內的資料，例如客戶姓名及信用卡號碼等。

一般保安預防措施
要有效防止被安裝鍵盤側錄程式，在日常使用電腦時，你應注意各項網上安全措施，例如：
※ 避免使用公共電腦進行涉及敏感資料的活動，如網上銀行服務。
※ 不應瀏覽可疑或不可信賴的網站，或從網站中下載程式及軟件。
※ 不應開啓來歷不明的電郵及其附件。
※ 選擇設有使用雙重認證，如智能卡及密碼登入功能的網上服務或系統。
※ 在使用便攜式電子裝置前，預先用防毒軟件掃描該裝置。

另外，你必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件(Anti-malicious Code Software)如防毒軟件，並須安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，以及啓動相關軟件的「自動更新」功能。

考考你
1. 鍵盤側錄程式是否可用作擷取輸入鍵盤的活動？

2. 以下哪一些是鍵盤側錄程式入侵後的威脅？
I) 利用電郵信箱來濫發電郵及散播電腦病毒
II) 偷取電腦內儲存的資料
III)收到廣告電郵
A) I & II
B) I & III
C) I，II & III

22－ 勒索軟件

爲了敲詐金錢，入侵者會設計一些勒索軟件在互聯網上發放，如果用戶的電腦無意間被植入這些軟件，用戶的電腦或內聯網上所有的特定檔案，如文件檔、試算表、數碼相片等會被加密。跟著，入侵者會向受影響用戶勒索金錢，除非用戶向入侵者交贖金購買解密程式和解密鑰匙，否則不能打開已被加密的檔案。

感染途徑
用戶電腦通常透過用戶的以下行爲，而在不知情下被植入勒索軟件，包括:
※ 瀏覽可疑網站；
※ 安裝或開啓來歷不明的檔案或軟件；
※ 開啓來歷不明的電郵及其附件。

保安措施

由於勒索軟件是頗複雜的惡意軟件，因此我們必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件，如防毒軟件，並須安裝防火牆和最新保安修補程式，每周最少全面掃描電腦一次，以及啓動相關軟件的「自動更新」功能，以防範勒索軟件的入侵。
重要的文件亦應該定期備份，如有必要，可增加備份次數，以確保最新的資料受到保護。
應時常保持自己的資訊保安意識，切勿從不知名的網站下載和安裝軟件。

應避免瀏覽可疑網站，例如在濫發電郵內提供連結的網絡遊戲、網絡賭博或社交網站等。
除了基本的保安措施外，亦應制定以防萬一的應變方案，以便一旦受到勒索攻擊時，可冷靜地根據程序作出適當的應變行動。

考考你
1.下列哪項能防範勒索軟件入侵？
A) 安裝反惡性程式碼軟件
B) 瀏覽可疑網站
C) 安裝來歷不明的檔案或軟件

2. 有效的資料備份是否能將受勒索軟件加密的資料還原？

23－ 殭屍電腦及殭屍網絡

什麼是殭屍電腦？
「殭屍電腦」是指一部連接著互聯網，並在用戶不知情下被攻擊者入侵及遙距操縱的電腦 。

什麼是殭屍網絡？
「殭屍網絡」是指由大量殭屍電腦所組成、並已遭攻擊者接管及遙距控制的網絡。攻擊者會透過一些電腦指令和控制中心操控殭屍網絡，作非法活動。

如何變成殭屍電腦 ？
你的電腦在甚麼情況下，可能會變成殭屍電腦？
若你的電腦被植入惡性程式碼(Malicious Code)，如特洛依木馬(Trojan Horse)，電腦便會被攻擊者操控，可能變爲殭屍電腦。

受感染的徵兆
變成了「殭屍電腦」後，通常會出現以下的徵兆：電腦可以如常運作及功能看似正常，不會癱瘓。電腦運作的速度會減慢、網絡負擔會增加，電腦亦可能出現來歷不明的檔案或執行一些來歷不明的程式。

潛在的保安威脅及影響
攻擊者通常遙距及隱蔽地控制殭屍網絡內的殭屍電腦，並利用這些電腦在互聯網上進行惡意活動，包括：

※ 濫發電郵
※ 攻擊其他電腦與伺服器

攻擊者可控制殭屍網絡中數萬台的殭屍電腦，同時向同一目標發動大規模的攻擊，使攻擊目標癱瘓，並且引發「拒絕服務」。對網絡保安方面或保護使用者資料方面都造成極大的威脅。

一般保安預防措施
要避免成爲殭屍電腦：
※ 應注意各項網上安全措施，例如：
  ☐ 切勿開啓或回覆任何來歷不明或可疑的電郵，並應把它們刪除。
  ☐ 開啓電郵附件時要提高警覺。
  ☐ 不要登入可疑網站、點擊網站內的連結、或從網站中下載檔案或軟件
※ 若發現電腦出現異常情況，你的電腦可能已受惡性程式碼感染，或已成爲殭屍電腦。
※ 請切斷網絡連線，然後立即檢查及使用防毒軟件掃描電腦。
※ 另外，你必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件(Anti-malicious Code Software)如防毒軟件，並須安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，以及啓動相關軟件的「自動更新」功能。

殭屍電腦分佈廣泛，要偵測殭屍網絡有一定困難。各互聯網服務供應商、跨國執法機關或保安事故協調中心必須共同合作，才有機會找出隱藏在背後的攻擊者。

考考你
1. 「殭屍網絡」是否指由大量殭屍電腦所組成的網絡？

2. 攻擊者遙距控制網絡內的殭屍電腦後，會在互聯網上進行哪些惡意活動？
I) 散播病毒
II) 濫發電郵
III) 攻擊其他網站
A) I & II
B) II & III
C) I，II & III

24－ 網頁竄改

「網頁竄改」(Web Defacement)是一種常見的網絡攻擊，指網站內容(通常是主頁)遭未獲授權的竄改，變成了由入侵者發放的惡意訊息，一般的目的是要讓人知道該網站已被入侵。遭竄改了的網頁，可能有部分內容被更改，也可能整個網頁被換掉。

入侵途徑
入侵者會透過甚麼途徑去竄改網頁？

入侵者只要發現網站出現保安漏洞，便可利用專門設計的入侵工具，攻擊這些網站。例如：入侵者會利用網站伺服器操作系統的保安漏洞，或網頁程式編寫漏洞，執行特定程式，入侵伺服器，取得網站系統上的控制權，然後破壞網站。因此，系統內所有不需要的程式特權，必須全部刪除，減低系統若被入侵時所受的影響。

潛在威脅

如果網頁被竄改，你會面對甚麼威脅？

※ 若網頁內容被竄改，該網頁可能會發放一些虛假的訊息，誤導網頁瀏覽者，破壞機構形象及聲譽，甚至引致金錢損失。

※ 此外，其他的網頁內容如連結，可能也會被入侵者暗自竄改，將瀏覽者導入另一個惡意網站，通過下載及安裝惡性程式碼(Malicious Code)如特洛依木馬(Trojan Horse)，企圖入侵瀏覽者的電腦。

一般保安預防措施

防止網頁被竄改要注意什麼？

你的網站應採取多項預防措施，例如：

※ 根據供應商及機構內的保安指引，安全地配置網站伺服器。

※ 使用嚴格的密碼。

※ 傳送、處理或儲存數據時，將敏感的數據加密。

※ 定期爲程式與資料備份。

※ 每天檢查電腦系統和網站伺服器的記錄。

※ 定期執行保安評估及審計。

另外，你必須爲網站伺服器採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新保安修補程式，每週最少全面掃描伺服器一次，以及啓動相關軟件的「自動更新」功能。

考考你

1. 一般入侵者竄改網頁的目的，是否要讓人知道有關網站已被入侵？

2. 以下哪一個是被竄改了的網頁通常會出現的現象？

I) 網頁出現惡意訊息

II) 未能瀏覽該網頁

III)網頁圖片遭到未獲授權的更改

A) I & II

B) I & III

C) I，II & III

25－ 代碼插入攻擊

代碼插入攻擊是指透過在電腦程式或系統上插入代碼，干擾程式或系統的正常運作，從而構成保安威脅。攻擊者通常針對較易受攻擊的輸入檢驗程序入侵目標系統。

代碼插入攻擊例子(Structured Query Language)
最常見的代碼插入攻擊是互聯網上的SQL插入攻擊，這種攻擊可導致敏感數據泄漏、資料被更改或刪除，此外攻擊者可繞過身份驗證並成功地以他人身份連接到系統。

SQL 指令可透過網上應用程式查詢資料庫的資料。如果網上應用程式沒有驗證所有輸入的 SQL 指令參數是否有效，攻擊者便可利用程式設計的漏洞，更改或加插對系統構成威脅的 SQL 指令內容，甚至逃避存取控制，繞過身分驗證和權限檢查，再作進一步攻擊。

另外一種常見的代碼插入攻擊是跨網址程式編程攻擊(Cross Site Scripting，XSS)，攻擊者針對網上應用程式的保安漏洞，暗中更改網站手稿程式(Script)，進行竄改網站、植入電腦蠕蟲等破壞行爲。

保安措施
以人手審查程式碼或遵守嚴謹的程式編碼要求是比較有效的防範方法，舉例說：
1. 使用最小權限原則，例如避免使用管理員權限來執行應用程式，使其因未獲授權而無法修改系統檔案；
2. 程式源碼內不應含有任何密碼；
3. 進行數據輸入核對，例如限制可輸入的內容或核對所有用戶輸入的資料。

另外，應針對用戶輸入、存取控制、配置管理、介面、認證與作業系統等領域審查電腦程式或系統，評估這些領域的風險，以及潛在的保安漏洞。

使用保安審計工具，定時或即時掃描應用程式，一般都可以減低代碼插入攻擊的可能性。

考考你
1. 下列哪項不是常見的代碼插入攻擊手法？
A. SQL 插入攻擊
B. 代碼插入攻擊
C. 社交工程攻擊

2. 下列哪項是針對代碼插入攻擊的保安措施？
A) 程式源碼內不應含有任何密碼
B) 進行數據輸入核對
C) 使用保安審計工具，定時或即時掃描應用程式
D) 以上皆是

26－ 跨網址程式編程(Cross site scripting)

跨網址程式編程是一種網上應用系統的保安漏洞，攻擊者會在網頁上輸入的數據內容中加入隱藏的電腦程式(Script)，待用戶的瀏覽器運行時，做出惡意的行爲，例如轉移目標網站至惡意網站，甚至在用戶毫不知情下植入特洛依木馬(Trojan Horse)。

除此之外，攻擊者還可以透過電子郵件，將事先編制的網頁連結寄給用戶。該連結表面上看似目標網站的網址，但卻暗藏攻擊者的惡意程式碼。當用戶點擊連結時，隱藏在網頁內的手稿程式便透過用戶的瀏覽器直接啓動，在用戶毫不知情下，取得他們的敏感資料。

預防措施
要減低跨網址程式編程攻擊所帶來的風險，機構或個別用戶也要採取適當的保安預防措施。
機構方面：
※ 應該遵守良好的網頁編程原則，設定及使用標準的驗證機制來驗證輸入的數據，例如網上應用系統只會接受符合特定格式的數據；
※ 必須建立對保安事故的偵測與監控、遏制及預防機制，對於任何可疑的系統入侵，應遵照保安事故處理程序與報告的指引方針採取跟進行動。

個別用戶方面：
※ 必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新的保安修補程式，每週最少全面掃描電腦一次，及啓動相關軟件的「自動更新」功能；
※ 瀏覽任何陌生網站前，應關閉瀏覽器中支援JavaScript 及ActiveX 的功能。

考考你
1. 下列哪項網上應用系統的保安漏洞，會允許在受害者的瀏覽器執行手稿程式，導致劫持用戶對話？
A) 跨網址程式編程
B) 視覺仿冒
C) 仿冒詐騙
D) 虛假網址

2. 關閉瀏覽器中支援JavaScript 及ActiveX 的功能可以有效地減低跨網址程式編程攻擊所帶來的風險？

27－ 存取控制保安(Access Control Security)

存取控制保安，是一個分辨電腦系統用戶身分的機制。它也審核用戶在系統中的存取權限，以防止系統被未獲授權者入侵，以確保系統所處理資訊的機密性、完整性及可用性。

數據接達權限(Data Access Right)
數據接達權限須按照「需要知道」的原則，賦予用戶不同權限來存取資訊。

邏輯存取控制(Logical Access Control)
邏輯存取控制是一項保安措施，以「AAA」原則，通過認證(Authentication)、授權(Authorisation)及會計(Accounting)，確保資訊不會落在不恰當身分的用戶手上。

認證
認證系統的嚴密程度取決於個別電腦系統的不同要求，認證系統可利用不同認證方法，例如密碼、數碼證書等替用戶認證，目的是辨認進入者的身分，同時記錄審計追蹤作審計之用。

限制用戶連續登入失敗的次數，及延長用戶登入失敗後鎖定的時間，可以減低入侵者以暴力攻擊的方式，嘗試用不同密碼登入系統的風險。

密碼管理
密碼是登入電腦系統的其中一個關鍵，因此必須好好保護密碼及不可隨便交給他人。在系統存放及傳送密碼時，應通過加密處理。一般設定密碼的原則是「易記難猜」，例如「1+Tw0Eq3」。不應直接使用字典中可找到的文字。需要定期更改密碼。制定密碼組成的標準可以提高密碼的強度，使其不容易被破解。

會計
會計是透過審計追蹤把電腦系統日常運作的事件記錄下來，以便監控人員或程式可審核及翻查系統中的不尋常事件。現時一般較完善的應用系統大部分都已內置審計追蹤功能。

由於電腦系統的日常記錄可以十分龐大，審計追蹤功能應設定爲只集中記錄系統內不尋常的事件。否則全部記錄可能會佔用過多的系統資源，反而令真正不尋常的事件不易被發現。

審計記錄必須正確無誤，可供審核人員定期查閱。完整性對會計十分重要。一旦發現記錄不全或有任何不當行爲，必須立即報告及進行調查。

考考你
1. 除機密性和完整性外，以下哪一項也是存取控制保安必須考慮的重要保安範疇？
A) 可用性
B) 專業性
C) 方便性

2. 下列哪項是設定密碼的最佳做法？
A) 使用易記難猜的密碼
B) 使用配偶的出生年月日作爲密碼
C) 使用電話號碼作爲密碼

28－ 實體保安(Physical Security)

實體保安一般是有關系統的場地準備、設備保安及實體接達控制，通過內務管理及適當員工培訓提高保安水平，以減低天災及人患所造成的影響。

場地準備

實體保安首要處理的是場地準備。由於大部分重要的資訊科技設備，一般都放置在伺服器室內，故此伺服器室的場地準備工作必須慎重其事。場地準備工作一般包括以下幾方面：

(1) 伺服器室的選址及其保安規格；
(2) 「風」即是空氣調節、「火」即是火警控制 ；
(3) 「水」即是水患控制、「電」即是電源供應；
(4) 伺服器室進出監控機制。

內務管理

制定伺服器室及系統操作指引。例如伺服器室內要保持清潔，嚴禁吸煙和飲食。風、火、水、電等設施要定期進行維修及測試；定期檢查緊急出口，確保逃生通道無阻；危險或易燃物品應放置在安全位置；滅火器應放在伺服器室適當位置。

必須定期進行火警演習，使相關員工熟習火警發生時的應變程序。當使用及存放便攜式電子裝置時，必須選擇安全及適當的地方處理，以免資料外泄。

設備保安

設備保安一般是指電腦硬件或設備在運作時及棄置時的相關保安措施，包括：

※ 定期檢查資訊科技設備的狀況。
※ 替重要資料備份，並把備份媒體存放在與設備所在地保持一段安全距離的地方。如未經授權，不得存取備份媒體。
※ 放置媒體的運載箱，須具備一些實體保安功能，例如防火、防水、防磁等。
※ 在棄置或再用電腦設備時，應確保所有敏感資料已被徹底刪除。

實體接達控制

處理敏感資料的範圍，必須嚴禁閒人接近。可考慮使用實體接達控制來限制出入，例如使用密碼等，只准獲授權人士進入。出入記錄亦應定期審核及小心備存。

各項維修工作必須妥善記錄，並監督外來人員施工。

考考你

1. 實體保安是否一般包括有關資訊系統的場地準備、內務管理、設備保安及實體接達控制？

2. 用於運載備份媒體的運載箱應具備以下哪種實體保安功能？

A) 防水(Waterproof)

B) 防磁(Anti-magnetic)
C) 防火(Fireproof)
D) 以上全部皆是

29－ 數據保安

數據保安是指透過將數據加密及設定用戶檢視權限，防止未獲授權的人士存取相關數據。
對一般機構而言，在數據保安方面應注意以下幾點：
※ 數據分類(Data classification)
※ 數據及檔案加密(Data and file encryption)
※ 數據備份及復原(Data backup and recovery)
※ 棄置資料(Information disposal)

數據分類
在實施數據保安措施之前，所有資料必須根據資料的敏感程度和重要性分類，例如：一般資料、限閱資料、機密資料等。將資料分類後，因應保密類別的不同保安要求，制定相應的保護措施。員工一般要獲得授權，才可存取各類保密資料。

數據及檔案加密
數據加密(data encryption)是指把一些明確易讀的訊息，轉變爲一堆不能辨認及難以理解的文字，以加強數據和檔案在傳輸及儲存時的機密性。

數據備份及復原
設置有效的備份(backup)系統，以便在系統故障、資料被意外刪除或非法竄改時，可恢復(recover)原有的數據，以確保資料及軟件的可用性及完整性。
另外，應同時採取審計追蹤及網絡保護等措施，進一步加強資訊保安。

棄置資料
在棄置或再用儲存媒體之前，必須採用安全刪除的方法，將儲存媒體內所有資料及數據徹底清除，以免外泄。

安全刪除一般包括使用安全刪除軟件(secure deletion software)、消磁(degaussing)或實體銷毀(physical destruction)等方法。

考考你
1.下列哪項並不關於數據保安？
A) 數據分類
B) 數據及檔案加密
C) 數據分析
D) 數據備份及復原

2. 有效的資料備份是否可以確保資訊的完整性和可用性?

30－ 網絡及通訊保安(I)

網絡及通訊保安(Network and Communication Security)主要是防止惡意入侵對電腦網絡造成的破壞及滋擾，目的是保護網絡上的資訊。

相關的保安措施，一般包括：網絡保安控制(Network Security Control)、互聯網保安(Internet Security)、電郵保安(Email Security) 、無線網絡保安(Wireless Network Security)及網絡通訊的防範措施(Preventive Measure of Network Comm'n)等。

網絡保安控制
網絡保安控制通常包括一些基本的保安措施，如網絡入侵防禦系統(Intrusion Prevention System，IPS)、防火牆及防毒軟件等。

如內聯網絡需要連接外來網絡，可考慮安裝防火牆或網絡入侵防禦系統，以監控資料的流動，以及偵測和防禦網絡中的不當行爲。如偵測到外來攻擊活動，防禦系統應立即發出警報及作出回應，盡量減低對網絡服務帶來的不良影響。

防火牆是一個或一組系統，執行訊息出入控制政策，分隔內部及外部網絡，准許或拒絕網絡間的數據通過，防止外人在未獲授權的情況下連接到內部資訊系統。

此外，要特別小心保護敏感資料。在網上傳輸敏感資料前，必須將資料加密，更應實施保密插口層(Secure Sockets Layer，SSL) 、虛擬私有網絡(Virtual Private Network，VPN)等適當的保安措施。

網絡之間或電腦之間的通訊，均須通過互相認證。

互聯網保安
用戶須遵守機構所制定的正確使用互聯網服務守則或相關指引，例如：
※ 電腦瀏覽器必須配置正確，防止惡性程式碼如電腦病毒下載至電腦。
※ 不應使用網頁上的自動輸入密碼/密碼記憶選項來儲存密碼。
※ 切勿瀏覽可疑網站或從中下載檔案。
※ 應小心使用網上即時通訊或聊天室，避免電腦病毒經這些途徑入侵。

電郵保安
使用濫發電郵過濾及防毒軟件來過濾可疑或含電腦病毒的電郵，或可考慮應用認證、加密及數碼簽署等保安選項。

考考你

1. 網絡保安控制不包括下列哪項？

A) 網絡入侵防禦系統(IPS)

B) 防火牆

C) 防毒軟件

D) 鍵盤側錄程式

2. 防火牆被用於分隔內部及外部網絡，防止外人在未獲授權的情況下連接到內部資訊系統？

31－ 網絡及通訊保安(II)

無線網絡(Wi-Fi)透過大氣電波傳送資訊，任何人均可接收到在無線網絡中發出的訊號，入侵者更有機可乘從中截取訊息。所以，機構或個人必須好好保護無線網絡設備及傳輸的訊息，防止通訊資料被竊取。

此外，機構應實行嚴格的實體保安控制及用戶身分核對，控制無線訊號的發射範圍，只供已獲授權用戶連接，避免未獲授權人士輕易接駁上機構的無線網絡。
爲確保機密性，經無線網絡傳輸的訊息必須加密。機構應採用較強的無線網絡保安規約及加密算法，例如選擇WPA 或WPA2 規約，並採用高級加密標準AES。

網絡通訊的防範措施
入侵者可透過通訊網絡竊取敏感資料，更可利用網絡的保安漏洞入侵資訊系統。要保護電腦網絡，必須採取有效的保安措施，如定期覆檢網絡保安漏洞、安裝最新的保安修補程式等。

某些情況下，用戶可能需要透過機構提供的電腦網絡，連接機構內部的網絡及系統。機構必須對這些電腦網絡實施適當的保安措施，如用戶身分核對、權限控制等。
另外，用戶應盡量避免使用網吧或其他公共上網設施的電腦連接機構內部系統，因公共電腦可能已被其他使用者值入惡性程式碼如鍵盤側錄程式(Keylogger)，用戶的個人資料可能會因此被記錄及竊取。

如有需要透過互聯網連接至機構內部網絡，就必須採取適當的保安措施，例如使用虛擬私有網絡(Virtual Private Network，VPN)、保密插口層 (Secure Sockets Layer，SSL)等，以保護傳輸的資料。

虛擬私有網絡是透過一種稱爲「加密隧道」的技術，將發送者和接收者之間傳輸的資料加密，在網絡上建立安全連接。

保密插口層是一個保安規約，主要是保護在互聯網上傳送的數據。現時一般互聯網瀏覽器都能支援SSL 技術，以便傳輸敏感數據時能提供保護。

考考你

1. 下列哪種方法可以加強無線網絡保安？

A) 實體保安控制
B) 用戶身分核對
C) 爲無線網絡加密
D) 以上全部皆是

2. 虛擬私有網絡是否能夠爲發送者和接收者之間傳輸的資料加密，在網絡上建立安全連接？

32－ 資訊保安風險管理

世上任何機構的電腦系統，即使已有良好保安設施，也可能存在一些未被發現的保安漏洞，因而產生一定的保安風險，或會對機構造成損失。

資訊保安風險管理(Information Security Risk Management)就是要盡可能找出這些潛在問題，並作出補救，盡可能減少整個系統存在的風險。

風險分析

風險分析(Risk Analysis)是一套風險管理工具，當中包括以下步驟：(1) 資產確認與估值；(2)評估保安威脅； (3)分析潛在風險；及(4)提出建議以減低風險及所構成的影響。分析後的結果會被用作制定一個最可行的改善方案。由於最理想的方案一般成本較高,管理人員要在成本與效益間取得平衡。

一般風險管理在處理風險時大致有四種方法：

(一) 降低風險

在不影響業務正常運作的前提下，將電腦系統存在的風險減至最低。例如避免手提電腦給他人偷取，電腦在不使用時可放在有鎖的櫃內，妥善保護。

(二) 轉移風險

將部分或全部風險轉移給另一方，例如替系統購買保險，將部分承受的風險轉移給保險公司。

(三) 接受風險

權衡風險的高低與所構成損失的大小後，最後決定接受風險所帶來的潛在影響，而不就保安措施作出任何改動。例如沒有儲存敏感資料的手提電腦，其損失資料的風險有機會被接受。

(四) 避免風險

終止具有潛在風險的相關做法，以避免風險發生。例子是放棄使用手提電腦而只使用桌上電腦，以免因遺失手提電腦而造成損失。

保安風險評估及審計

保安風險評估通常會在新的資訊系統投入生產前進行，以及在推出後定期進行，評估結果及改善建議應以文件妥善記錄，以供保安審計覆檢之用。保安審計是一項以保安政策爲標準，定期覆核保安系統的程序，確保適當的保安措施已切實執行。

保安風險評估必須在當系統有重要變動時或按保安政策指定的時間重新進行。

考考你

1. 替系統購買保險是運用了以下哪一種處理風險的方法？

A) 接受風險

B) 轉移風險

C) 避免風險

2. 保安風險評估的結果及改善建議是否會用作保安審計覆檢之用？

33－ 資訊保安事故管理

資訊保安事故是指電腦資料外泄或對資訊系統的可用性、完整性和機密性構成威脅的事件。

保安事故處理是一系列持續進行的程序，包括：:

※ 事故發生前 - 規劃及準備(planning and preparation)；

※ 事故發生時 - 保安事故應變(response to security incident)；

※ 事故發生後 - 事後跟進(aftermath)。

規劃及準備

保安事故的處理工作，首要是全面規劃，並制定適當程序及具體執行指引。主要工作包括：

(一) 保安事故處理計劃(Security incident handling plan)

界定處理範圍、目標和優先處理事項等。

(二) 報告程序(Reporting procedure)

訂立報告可疑活動時的步驟和程序，以便及時通知參與事故應變工作的全體人員。

(三) 升級處理程序(Escalation procedure)

事先編備有關法律、技術和管理事項的決策人聯絡名單，以便事故發生時可迅速上報有關人士，確保立即落實相應的行動。

(四) 保安事故應變程序(Security incident response procedure)

訂明發生事故時應採取步驟，例如調查事故肇因、將破壞減至最少、使系統恢復正常操作等。

(五) 培訓與教育(Training and education)

各人員應熟習事故處理程序，包括事故報告、確認和採取適當行動以恢復系統正常操作。

(六) 事故監察措施(Incident monitoring measure)

安裝入侵偵測工具，主動監察、偵測，並就系統入侵作出應變。

保安事故應變

保安事故應變是指發生事故時須即時採取的應變程序，以盡快恢復系統的正常操作狀態。

保安事故應變一般可分爲以下五個階段：

(一) 確認(Identification)：

※ 判斷是否確實發生事故；
※ 進行初步評估；
※ 記錄事故和系統當前狀況
(二) 升級處理(Escalation)：
※ 通知有關人士，以尋求協助及指示。
(三) 遏制(Containment)：
※ 控制受影響範圍和將受損程度減至最低；
※ 保護重要的資源；
※ 決定是否須暫停系統操作，例如暫時關閉或隔離受襲的主機或系統，以防止事故對互相連接的其他系統造成破壞。
(四) 杜絕(Eradication)：
※ 杜絕是指從電腦清除導致事故的肇因，例如從受感染的電腦和媒體清除電腦病毒、通過安裝修補程式/修復程式堵塞保安漏洞、糾正系統不當配置和更換密碼等。
(五) 復原(Recovery)：
※ 復原受損或遺失資料；
※ 恢復系統正常操作。

事後跟進
發生保安事故後，應採取跟進行動，評估事故的發生原因，並加強保安措施，以防止同類事故再發生。

跟進行動包括：
※ 事後分析(post-incident analysis)；
※ 事後報告(post-incident report)；
※ 保安評估(security assessment)；
※ 覆檢現行保護措施(review on existing protection measures)；以及
※ 調查和檢控(investigation and prosecution)。

考考你
1. 下列哪項不是在發生保安事故時所採取的「應變行動」？
A) 培訓與教導
B) 升級處理
C) 遏制
D) 杜絕

2. 下列哪項是保安事故處理的主要步驟？
A) 規劃及準備
B) 保安事故應變
C) 事後跟進
D) 以上全部皆是

34－ 應用系統保安

應用系統(Application system)是一套根據用戶要求編寫出來的電腦程式。

應用系統保安(Application security)主要是爲用戶提供安全的操作環境。除了系統上的保安措施外，應用系統亦應添配適當的保安措施，以堵塞應用系統本身的保安漏洞和加強保護系統所處理的敏感數據。

有關發展及維修應用系統的資訊保安，分別有以下幾個範疇：
(一) 系統規格及設計控制(System specification and design control)
(二) 程式編製控制及人員安排(Programming control and personnel arrangement)
(三) 程式/系統修改控制(Program/system change control)
(四) 程式/系統測試(Program/system testing)

系統規格及設計控制
在應用系統的開發階段，必須確保系統的設計符合保安要求及規格。
系統開發組、資料擁有者和用戶應根據數據的敏感性和重要性，共同決定系統的保安要求。其中包括設定適當的審計政策、共同覆檢程序、確保資料機密性及完整性的方案和制定應變計劃等。

程式編製控制及人員安排
程式編製控制是指制訂程式編寫標準，以確保程式編製員遵守發展和維修程式的保安標準及規格。

對於要處理敏感資料的應用系統來說，一般是根據職務分工(segregation of duties)來劃分操作人員及程式編製員的職責，將重要功能的各個步驟分別交由不同人員處理，以免重要程序因集於一人手上而被破壞。

程式/系統修改控制
應用系統在運作過程中，難免會因應新的需求或保安漏洞而須要修正，而程式/系統修改控制的目的就是制定修改的原則及規格，並通過適當的審批程序，確保在修改過程中維持系統的完整性，防範惡意竄改行爲，減低欺詐及出錯等潛在風險。

程式/系統測試
程式/系統測試除了針對應用系統的可用性及可靠性進行測試外，還要對資訊保安控制進行測試，這樣才可有效減低應用系統出現保安漏洞的機會。
例如，針對網上應用系統所有輸入參數的驗證程序作出測試，確保這些驗證程序能有效防止代碼插入攻擊和跨網址程式編程攻擊。

考考你

1. 職務分工是否指在劃分職責時，將重要工作的各個步驟交由同一人員處理，以減低重要程序被破壞的可能性？

2. 程式/系統修改控制是否通過已建立的修改要求及審批程序，來維持系統的完整性，並減低系統被未獲授權竄改的風險？

35－ 網上應用系統保安

網上應用系統由電腦程式組成，在網站伺服器上執行。伺服器透過連接後端數據庫，以超文本傳輸規約(HTTP)回應客戶端動態網頁的要求，在互聯網或內聯網提供各種跨平台服務。例如進行電子交易時，用戶會在網頁輸入有關資料包括信用卡號碼，便可完成該項交易。

網上應用系統的保安威脅

由於網上應用系統通常已連接互聯網或內聯網，用戶不但可以有效地使用該系統提供的資源，也能夠提升工作效率。不過，網上應用系統也同時帶來一定的保安威脅。

網上應用系統的保安威脅一般源於：

(一)不可靠的客戶端

由於網上應用系統通常不能監控遠端用戶的操作，因此系統設計不應完全信任並直接處理客戶端所輸入的資料。

(二)網上應用系統設計上的保安漏洞

攻擊者針對應用系統設計上的保安漏洞來攻擊系統，常見的攻擊包括代碼插入攻擊(code injection attack)和跨網址程式編程攻擊(cross site scripting attack，XSS)等。

(三)不安全的網絡通訊

如果網上應用系統與客戶端之間是透過互聯網或其他不安全的網絡來傳輸沒有加密的資訊，資訊便有可能在傳送過程中被讀取及更改。

保安措施

機構設計網上應用系統時，應採取適當的保安措施，以減低保安風險。保安措施通常可分爲以下各個範疇：

(一) 網上應用系統保安參考結構

網上應用系統結構一般包括三個層級：對外網站伺服器、應用系統伺服器及數據庫伺服器。有了這些層級結構，即使攻擊者可入侵對外網站伺服器，仍須另尋方法攻擊內部網絡。對外網站伺服器應置於非軍事區(demilitarised zone，DMZ)內。非軍事區是一個特別網絡區域，內設伺服器，可接達互聯網服務。儲存敏感資料的伺服器則應設於內部網絡，受額外保護。

(二) 網站伺服器軟件保安指引
網站的系統管理員須按網站伺服器軟件保安指引，適當地配置網站伺服器及存取權限。例如避免使用特別權限帳戶(如「root」、「SYSTEM」、「Administrator」)來執行網站伺服器程序，使網站伺服器軟件無法修改未經授權的系統檔案。以及採取適當措施例如使用保密插口層(secure sockets layer，SSL)，將傳輸的資料加密。

(三) 網上應用系統發展程序
在發展軟件初期，便須分析及界定網上應用系統的保安控制。例如檢視程式源碼，找出於開發階段忽略了的保安漏洞。此外，進行風險測試也有助減少常見的程式保安漏洞。

(四) 網上應用系統安全編碼
軟件發展小組應根據一些網上應用系統安全編碼作業實務，例如驗證所有輸入參數的有效性，並過濾輸入內容中的特殊字符如~!#$%^&*[]<>，以有效防止代碼插入攻擊和跨網址程式編程攻擊。

考考你
1. 下列哪項保安威脅會在網上應用系統上出現？
A) 不可靠的客戶端
B) 網上應用系統設計上的保安漏洞
C) 不安全的網絡通訊
D) 以上皆是

2. 透過驗證輸入內容的輸入參數及過濾特殊字符，是否可以防止代碼插入攻擊和跨網址程式編程攻擊？

36－ 保安風險評估及審計

保安風險評估(Security Risk Assessment)是一個程序，以確認可能影響資訊資產保安的風險、弱點和威脅，加以分析及了解，以制定所須的保安措施。

保安風險評估程序一般包括確認和分析：
1. 系統上所有資產；
2. 可影響系統機密性、完整性或可用性的威脅(Threats)，例如惡性程式碼的散播和未經授權的資料存取等；
3. 可能受到威脅的系統漏洞(System Vulnerabilities)，例如沒有替軟件安裝最新的系統修補程式；
4. 威脅帶來的潛在影響(Impacts)及可能發生的機會率和風險 (Risks)；
5. 控制風險所須的保護措施，例如加強保護網絡構件和設備及更新相關系統的設定；
6. 適當保安措施的選擇及它們與風險的關係。

保安審計

保安審計是一個程序，以該機構的保安政策及其他保安標準爲基礎，測定現行保護措施的整體狀況是否達到所須的標準。

保安審計程序

保安審計程序主要包括以下步驟：

※ 制訂審計範圍–編製審計清單，內容可能涵蓋網上應用系統、網絡結構、無線網絡等各個領域。

※ 查找保安漏洞–通過保安審計工具和不同的技術找出潛在的保安漏洞。例如:利用滲透測試(Penetration Testing)，針對有可能的入侵途徑，找出網絡和系統中潛在的保安漏洞和弱點。

※ 提出改善建議–完成審計後，編寫一份審計報告，比較現有的保安措施與保安政策及標準之間的差異，並提出改善建議。

保安風險評估及審計跟進

保安風險評估和審計雖然可爲機構分析及評估保安風險，並提出適當的改善建議，但更重要是機構有效地落實執行這些改善措施。

建議提出後，如管理層決定不依建議執行，就必須提出充分理由及承擔日後相關的保安風險。

考考你

1. 保安風險評估是否用來評估使用資訊科技相關之保安風險？

2. 下列哪項不是資訊科技保安的審計步驟之一？

A) 制訂審計範圍
B) 查找保安漏洞
C) 爲數據備份
D) 提出改善建議

37– 資訊科技服務外判保安(IT outsourcing)

是將部分或全部資訊科技服務或功能外判予第三方服務供應商，目的是減省成本及專注發展核心業務，機構還可以利用獨立及專業人士的專業服務，幫助自己完成本身不太擅長的工作。

資訊科技服務外判可以涵蓋各種不同服務範疇，例如應用程式的開發和維修、網絡管理、桌上電腦管理、資訊科技服務支援熱線及數據中心的操作等。

資訊科技服務外判的風險

外判供應商有機會處理機構內敏感和重要的資料，對機構造成以下的保安風險：

1. 供應商可接觸機構的基礎設備，甚至知悉系統內潛在的弱點和缺陷；

2. 爲提供服務，供應商可能獲發有效的用戶賬戶，以使用相關資料和系統，如人力資源管理系統，因而取得敏感或個人資料。

管理資訊科技服務外判
當外判資訊科技服務時，機構必須執行適當的保安管理程序來保護敏感或個人資料。以下是一些應該考慮的安全做法：
1. 所有由資訊系統處理的資料，應有明確和適當的保密級別分類，並按「需要知道」的原則給予存取資料的保安權限。

2. 外判服務供應商必須簽署不可向外披露資料協議(Non-disclosure Agreement)，確保它小心處理系統中的敏感數據，以防外泄。此外，外判合約亦須包括服務水平協議(Service Level Agreements)，列明各項保安控制的預期水平，並就任何經確認的違約行爲訂明補救及應變措施。

3. 定期監察和覆審服務供應商及用戶的保安控制遵行情況，也可以安排第三方人士進行獨立的保安審計。

4. 確保外判服務供應商有適當的資訊系統應變計劃及備份程序。
管理人員必須緊記，任何機構只能外判服務，但不能外判其責任。因此，管理人員應定期提高員工在資訊保安方面的認知，提供適當培訓，使他們擁有相關的保安知識來管理外判工作。

考考你
1. 下列哪項是資訊科技服務外判的風險？
A) 外判供應商有機會得到機構內的敏感資料
B) 供應商可能獲得有效的用戶賬戶作不軌行爲
C) 供應商知悉系統潛在的弱點和缺陷，可能作進一步攻擊
D) 以上皆是

2. 下列哪項是在管理資訊科技服務外判時須要考慮的安全做法？
A) 爲資料作出明確和適當的保密級別分類
B) 按「需要知道」原則給予存取資料的保安權限
C) 外判服務供應商必須簽署不可向外披露資料協議(Non-disclosure Agreement)
D) 以上皆是

38－ 資訊保安簡介

無論對個人或機構來說，資訊是一項重要的資產。資訊保安是指對資訊資產加以保護，以求達到機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)三項基本原則。

機密性一般是拒絕所有未經授權人士存取受保護資訊，避免資料外泄。最普遍的方法是通過

設定帳號和密碼，防止他人未經授權而進入電腦。另一個例子是將文件加密，以免資料內容在傳送及儲存過程中泄漏。

完整性是指禁止任何未經授權的刪改，確保資訊完整及準確。數碼簽署是一項常用的技術，用以確認資料的完整性，以免重要資料被竄改，而引致金錢及聲譽上的損失。

可用性是確保系統任何時侯均可正常運作，並隨時因應需求提供可用的資訊，例如設置後備電腦和設施，以及安裝能夠還原受損資料的備份系統等，確保資訊系統時刻保持順利運作。

資訊保安範疇一般包括以下部分：

實體保安(Physical Security)

實體保安是有關系統的實體管理措施，其中包括環境保安及設備保安。例如是以有鎖的電腦櫃保護載有資料的伺服器。

存取控制保安(Access Control Security)

存取控制保安是一套防止未獲授權人士使用系統的機制，以「AAA」原則，即通過認證(Authentication)、授權 (Authorisation)及會計(Accounting)程序，並按「需要知道」(Need-to-know)的準則處理資訊，以確保資訊不會落在不恰當身分的用戶手上。

數據保安(Data Security)

是要避免未獲授權人士披露、刪改或銷毀電腦資料，其中包括數據加密、數據備份等。

應用系統保安(Application Security)

應用系統保安是指達到對應用程式及測試環境的保安要求來保護資訊，其中主要包括系統修改控制、人員安排及程式測試。例如，根據職務分工(Segregation of Duties)來劃分操作人員及程式編製員的職責，以防止重要程序被一人破壞的可能性。

網絡及通訊保安(Network and Communication Security)

網絡及通訊保安是防止入侵者通過網絡造成破壞及滋擾。它主要包括監控電腦網絡、控制軟件安裝及防止電腦病毒在網絡上傳播。

保安風險評估及審計(Security Risk Assessment and Audit)

保安風險評估及審計是因應系統日常執行情況而定期檢測系統並跟進有關改善建議。

保安事故管理(Security Incident Management)

保安事故處理是資訊保安管理中重要的一環，在發生資訊保安事故時啓動適當程序，例子包括如何處理資料外泄事故等。

機構在資訊系統發展過程中都必須參考以上各個保安範疇，並因應實際情況不斷作出定期檢討和改善。

考考你

1. 以下哪項是指敏感數據受到保護，及只向獲授權一方披露？

A) 可用性

B) 機密性

C) 完整性

2. 實體保安是否在資訊保安範疇以內？

39－ 安全刪除

安全刪除是一種令已刪除的資料無法復原的方法，一般應用於刪除重要或敏感的數據。

在棄置或再用儲存媒體之前，就必須先將敏感資料徹底刪除。所謂的儲存媒體包括硬碟、光碟或便攜式儲存裝置等。同時，電腦或任何辦公室電子設備包括多功能打印機和影印機，如果有內置的儲存媒體，而又可能含有敏感資料，亦應用安全刪除的方法，將這些儲存媒體上的敏感資料徹底刪除，以免外泄。

刪除指令或格式化指令的原理

一般格式化 (Format) 和刪除 (Delete) 指令，其實只刪除檔案的位置指標，但檔案的內容會一直保留在原位，直至檔案所佔的空間被其他檔案使用。

市面上有一些復原軟件工具，可以復原因執行格式化或刪除指令而刪除的數據。

安全刪除的方法

安全刪除一般有三種方法：

※ 蓋寫 (Overwriting)

※ 消磁 (Degaussing)

※ 實體銷毀 (Physical Destruction)

蓋寫

蓋寫就是使用安全刪除軟件及服務，將儲存媒體上的數據，以隨機字符或一系列的0 和1(或類似的位元模式)重覆蓋寫多次，使原有的數據徹底清除。

在執行蓋寫前，務必正確設定軟件並確定在刪除過程中沒有出現錯誤，才能保証儲存在媒體內的數據被完全刪除。

消磁

消磁技術是以專用的消磁器 (Degausser)，以強大的磁場來徹底破壞磁性儲存媒體上的數據。若使用恰當，消磁可以完全清除令原本儲存於磁性儲存媒體上的數據並無法透過其他軟件或以實驗室的先進儀器還原。

除了清除數據所須的時間較蓋寫少，消磁技術亦特別適用於一些已損壞的硬磁碟機上。因損壞硬磁碟機往往無法進行蓋寫。

在消磁過程中，應小心遵照廠商的說明書操作，以免因處理不當而將大量資料殘留在磁性儲存媒體上。

實體銷毀
實體銷毀一般就是用切碎或打碎的方法來破壞儲存媒體。這方法適用於銷毀一些不能用蓋寫或消磁方式刪除的數據。

對於一些儲存了敏感資料的儲存媒體，除了使用蓋寫或消磁方法刪除資料外，亦建議在棄置前將媒體作實體銷毀，以策安全。

由於儲存媒體的技術不斷進步，以上的安全刪除方法只可用作參考。實際應用時，必須根據儲存媒體所用的技術選擇最有效的安全刪除方法。

考考你
1. 一般格式化和刪除指令是否會同時刪除檔案的位置指標及檔案的內容？

2. 下列哪種安全刪除方法是利用強大的磁場將磁性媒體上的數據消除？
A) 格式化(Formatting)
B) 蓋寫(Overwriting)
C) 消磁(Degaussing)

40－ 內容過濾

內容過濾一般是指過濾不恰當的資料內容或訊息，如載有不良資訊、個人或敏感資料的內容。在資訊保安方面，內容過濾功能可以應用在多個層面，例如瀏覽互聯網、接收電子郵件、檢視網上搜尋器的搜尋結果、存取數據庫資料等。

內容過濾功能的應用
家長可以利用內容過濾軟件，彙編和修訂不良網站資料庫，把不適合兒童及青少年使用的網站濾除，更可限制上網時間。這樣便可防止子女瀏覽不良的網上內容和沉迷上網活動。

此外，機構也可以使用內容過濾軟件，防止員工濫用資源，例如從互聯網下載大量檔案、瀏覽不良網站等，浪費機構的網絡帶寬和資源。
互聯網用戶可以選擇使用互聯網供應商提供的保安措施，例如電郵過濾服務，減少接收濫發電郵的數量。

如果機構設有電郵伺服器，亦可以安裝內容過濾系統，把收到的電郵先行篩選，過濾濫發電郵和受病毒感染的電郵，然後才送至個別員工的收件箱。內容過濾系統亦可以先檢查員工寄送的電郵內容是否含有敏感資料，才讓電郵經互聯網寄出，減低敏感資料外泄的風險。

內容過濾的運作

內容過濾一般有幾種做法，以下以過濾網頁內容爲例作簡單介紹。

1. 只允許用戶瀏覽「白名單」(White List)內的網站。白名單是一個儲存認可網站的資料庫，用戶的瀏覽器會檢查網站是否白名單內的認可網站，才讓用戶瀏覽。
2. 防止用戶瀏覽「黑名單」 (Black List)內的網站，這些網站通常含有不良成份，不適合用戶瀏覽。
3. 有些內容過濾工具附有供應商定期修訂的網頁內容分類資料庫，此資料庫根據既定的評分標準，對網頁內容作出分類及評分，以判別網頁內容是否適合瀏覽。
4. 有些內容過濾器結合以上多種不同的內容過濾方法，以提高準確性和效率。

其他相應最佳作業實務

雖然內容過濾可以提供上述保障，但是家長或機構仍須作出相應行動配合。家長可以多花時間與孩子一起瀏覽互聯網，指導他們良好的網上行爲。機構應定期爲員工提供適當的資訊保安培訓，提高他們對資料保護的意識。

考考你

1. 下列哪項名單載列了認可網站，以幫助用戶檢查網站是否適合瀏覽？

A) 白名單(White List)
B) 黑名單(Black List)
C) 紅名單(Red List)
D) 藍名單(Blue List)

2. 下列哪項名單載列了不良網站，以防止用戶瀏覽？

A) 白名單(White List)
B) 黑名單(Black List)
C) 紅名單(Red List)
D) 藍名單(Blue List)

41－ 數據加密

數據加密(Data Encryption)是指把一些明確易讀的資訊，轉變爲一堆令人不能辨認及難以理解的文本，藉此減低數據在儲存及傳送時，因資料外泄所帶來的重大損失。因此，數據加密是其中一個保護電腦數據的有效方案。

加密解決方案的主要組件

加密解決方案的主要組件有以下幾種：

※ 加密算法(Encryption Algorithm) 原理是利用數學算法產生一組密碼匙，以此進行加密及解密數據程序，常用的加密算法包括RSA、AES 等；
※ 密碼匙(Encryption Key)可分爲對稱密碼匙(Symmetric Key)及非對稱密碼匙(Asymmetric Key)兩種，對稱密碼匙是指以同一條密碼匙來加密及解密數據，可以用於數據儲存，例如AES 算法通常用於便攜式電子儲存裝置的數據加密。非對稱密碼匙則使用一組配對的密碼匙(Key Pairs)，方法是以其中一條密碼匙將數據加密後，必須以相配的另一條密碼匙方可將數據解密，應用例子有公開密碼匙基礎建設(Public Key Infrastructure)等；
※ 一般而言，若使用相同的加密算法，密碼匙長度(Key Length)愈長，所加密的數據就愈難以被強行拆解。

如何選擇加密解決方案
現時有一些應用程式或操作系統均附帶加密功能，准許文件擁有人以指定密碼，來限制其他使用者讀取加密文件。如果涉及到個人或敏感數據，我們需要選購較專業的加密軟件或支援硬件加密的儲存裝置去加密數據，這些軟件或裝置通常採用較強的加密算法如AES 及較長的密碼匙。

如有需要通過互聯網連接機構內部網絡，就需要建立「加密隧道」，例如使用虛擬私有網絡，將傳送過程中的數據加密。

加密的好處
加密技術主要是保護數據的傳輸及儲存，以加強其機密性。傳輸數據加密一般可用於電子商貿、無線網絡保安及遠程接達，藉以減低被竄改或竊取的風險。而儲存數據加密則適用於數據、檔案、電郵、甚至整個硬碟上。

隨著愈來愈多機構應用資訊科技，敏感資料在電子形式下泄漏的風險不斷增加，我們必須加深了解加密的方法並採用適當的加密解決方案，以減低數據外泄的風險。

考考你
1.哪項組件不是應用於以同一條密碼匙來加密及解密數據的加密解決方案？
A) 非對稱密碼匙 Asymmetric Key
B) 對稱密碼匙 Symmetric Key
C) 加密算法 Encryption Algorithm

2.一般來說，若使用相同的加密算法，密碼匙長度愈長，已加密的數據就愈難以被強行拆解

42－ 多層防禦

多層防禦(Defense in Depth) 是一種防禦機制，以多重的網絡保安結構對抗使用不同攻擊方法的入侵者。較單一的防禦機制更安全及牢固。

多層防禦的理念
多層防禦概念源自軍事領域。多層防禦的目的是拖延入侵者的攻擊，從而爭取更多時間作出軍事部署。

電腦網絡的多層防禦機制，就是一方面攔截入侵者攻擊電腦網絡，另一方面讓系統管理員騰出較多時間，爲系統作出檢查及修正，從而減低入侵者成功入侵的機會及其所帶來的影響。

多層防禦的設置和運作
以下是一個多層防禦設置的簡單例子：

多層防禦的設置一般會由機構內部網絡 (Internal Network) 對外連接其他網絡如互聯網的通訊閘口開始，一直伸延至內部伺服器及用戶電腦的安全設置。它通常包括兩層防火牆 (Firewall)、非軍事區(Demilitarised Zone，DMZ)、入侵偵測系統 (Intrusion Detection System，IDS) 和防毒軟件等。

守住整個網絡的先鋒是外部防火牆 (Outer Firewall)。外部防火牆，例如封包過濾防火牆 (Packet Filtering Firewall)，擁有抵抗外部網絡攻擊的前線防禦功能。它會依據定義好的規則，過濾每個流入或流出的封包 (Packet)，以確定是否允許或阻止封包的進出。

在兩層防火牆之間組成的非軍事區，把內部和外部網絡分隔，並讓允許外來網絡接達的伺服器，如網站伺服器 (Web Server)存放在這裏，避免外部網絡直接連接到內部網絡。

而非軍事區一般會設置入侵偵測系統，以偵測對非軍事區的攻擊。如發現有入侵的現象，入侵偵測系統會發出警報及報告，讓網絡管理員盡早發現攻擊而作出檢查及修正。

緊貼其後就是內部防火牆(Inner Firewall)。內部及外部防火牆應來自不同的供應商，以防止入侵者攻擊相同的潛在保安漏洞。

相比外部防火牆純粹地過濾封包，內部防火牆一般會進一步檢查資料封包的內容，並根據封包的來源和目的地 IP 位址、連接埠號碼及所要求的服務來決定提供或拒絕該網絡服務。

而再深入一層便到達內部網絡。內部網絡的伺服器及用戶電腦一般會設置包含最新病毒識別碼的防毒軟件及安裝了防火牆，作進一步的保護。

總括而言，即使外層有保安漏洞或缺失，令入侵者有機可乘攻擊網絡，下一層的保安設施也可作出適當的防禦及警報。

而每個保安層均設置不同功能及技術的保安措施，令入侵者在一般情況下難以入侵，以保護重要資訊。

考考你

1. 多層防禦是否比單一的保安措施更加安全？

2. 下列哪項通常不會被置於非軍事區(Demilitarised Zone，DMZ)內？

A) 入侵偵測系統(Intrusion Detection System)

B) 網站伺服器(Web Server)

C) 內部應用軟件伺服器(Internal Application Server)

43－ 端點保安

端點(Endpoint)一般指任何已連接至電腦網絡，並能夠儲存數據的電子裝置，包括桌上電腦、手提電腦、智能手機和便攜式電子儲存裝置(Portable Electronic Storage Device)等。

端點保安(Endpoint Security)是爲保護端點裝置及其儲存的資料而實施的保安措施，目的是：

※ 在所有端點實施最新的保安政策；

※ 確認、控制和管理抽取式裝置的使用；

※ 防止資料被複製至未獲授權的電子儲存裝置；

※ 強制加密電子儲存裝置上的資料；

※ 提供詳細的審計記錄；

※ 防止惡性程式碼如電腦病毒從端點裝置入侵機構網絡。

端點保安措施

端點裝置的種類不斷增加，其應用範圍亦逐步擴大，單靠一般的電腦保護措施，例如防毒軟件及個人防火牆等，並不足以保護這些裝置所儲存的資料。如要達到較完善的保護，便須採取由以下不同技術整合而成的端點保安解決方案：

數據加密(Data Encryption)

當資料傳送至抽取式裝置時，會自動被轉化爲看起來是無用及難以理解的數據，加強資料的機密性。

連接埠控制(Port Control)

通過建立適當的端點保安要求及規定，端點用戶會被允許或禁止使用端點裝置上不同的連接埠(Port)，例如禁止端點用戶透過USB 連接埠連接任何抽取式裝置。

裝置控制(Device Control)

端點裝置有不同的種類，如便攜式電子儲存裝置、光碟燒錄機和掌上電腦等。由於每個端點裝置一般都擁有獨特的裝置識別碼，裝置控制可透過註冊這些識別碼來授權用戶使用。

應用程式控制(Application Control)

應用程式控制是限制只有經授權的應用程式在端點裝置上執行。這樣可以避免用戶因不小心而安裝及執行未經電腦擁有者授權使用的應用程式，例如從互聯網上下載的免費軟件。

總括而言，端點保安措施可以加強保護每個端點裝置，防止入侵者對端點裝置的攻擊及減低資料外泄的機會。同時，機構亦應教育員工注意資訊保安，不應隨意從可疑網站下載檔案，包括應用軟件或軟件更新程式等。

考考你

1. 端點是否一般指任何已連接至電腦網絡，並能夠儲存數據的電子裝置？

2. 下列哪項保安措施通常是端點保安解決方案的其中一環？

A) 裝置控制
B) 應用程式控制
C) 數據加密
D) 以上全部皆是

44－ 公開密碼匙基礎建設(Public Key Infrastructure，PKI)

公開密碼匙基礎建設提供安全可靠的環境在互聯網上進行電子交易，這保安架構主要利用公匙加密技術來保障資訊的保密性、完整性、真確性及不可否認性。

核證機關與數碼證書

公開密碼匙基礎建設的有效運作十分依賴核證機關(certificate authority,CA)的支援。核證機關的主要工作是以一個可信靠的第三者身分來核證進行電子交易雙方的身分。

數碼證書是以電子形式發出的證書，其所儲存的數據可用以核實證書擁有人的身分。證書通常包含的資訊包括用戶的公開密碼匙、姓名及電子郵件地址等。

當註冊機關(registration authority，RA)核實申請人的身分後，核證機關便會向申請人發出一份經該機關數碼簽署的證書副本，並在公開目錄登記該申請人的公開密碼匙。

證書撤銷清單(Certificate Revocation List，CRL)是一份由核證機關定期發出的清單，清單上載列在屆滿日期前被撤銷或暫時吊銷的證書。在使用他人的公開密碼匙前必須核實該密碼匙是否有效，以防止無效的證書被濫用。

公匙加密技術

公匙加密技術涉及爲每個用戶提供一對密碼匙，分別是用戶自己保管而不可隨便向外公開的私人密碼匙(private key)，以及可以對外公開的公開密碼匙(public key)，這一對不同但互相配對的密碼匙將相關的數據加密，以確保訊息的機密性。例如，若使用公開密碼匙加密數據，只有使用與其相配的私人密碼匙才能解密。

以傳遞電子郵件訊息爲例，寄件人可以透過使用收件人的公開密碼匙，把要寄出的電子郵件內容加密。收件人收到電子郵件後，便一定要使用自己保管而與該公開密碼匙配對的私人密碼匙，才可把郵件解密。這樣便可以確保電子郵件內容的保密性。

另外，爲了確保該電子郵件的完整性、真確性及不可否定性，寄件人會將電子郵件的內容利用數學算法產生資訊摘要(message digest)，並以自己的私人密碼匙加密形成數碼簽署，然後將電子郵件連同數碼簽署發送給收件人。

當收件人收到電子郵件後，會利用寄件人相應的公開密碼匙核對該數碼簽署是否有效，以及以相同數學算法產生的資訊摘要，來核實該電子郵件是否有效。
這樣，收件人便可以肯定該電子郵件確實來自寄件人，確認該電子郵件的真確性和完整性；同時，寄件人亦不能否認曾經簽署該電子郵件，確保電子郵件的不可否定性。

考考你
1. 私人密碼匙是否可以隨便向外公開？

2. 證書撤銷清單是否指一份由核證機關定期發出的清單，而清單上載列在屆滿日期前遭撤銷或暫時吊銷的證書？

45－ 互聯網規約版本 6 的保安

什麼是互聯網規約版本6?
互聯網規約版本4 (Internet Protocol version 4，IPv4)是常見的互聯網通訊標準，它採用32 位元(bit)的位址，可提供的位址數目有限。隨着科技產品尤其是流動裝置數量的快速增長，可用的IPv4 位址不敷應用。

互聯網規約版本6(Internet Protocol version 6，IPv6)是新的互聯網通訊標準，採用較長的128 位元位址，它可提供的位址數目遠較IPv4 爲多。

IPv6 的保安特性
IPv6 在保安方面也作出改進，爲網絡提供更佳的保護，例如：
1. 互聯網規約保安(IPsec)被修改爲強制性的功能，可爲網絡傳輸提供認證，保持傳輸資料的完整性及保密性。

2. IPv6 位址可以跟已簽署的公開密碼匙連結在一起，允許使用者爲特定的IPv6 位址提供擁有權證明(Proof Of Ownership)，使仿冒和竊取IPv6 位址較爲困難。

3. IPv6 把位址擴充至128 位元，大大增加了位址空間，因而提供一道有效屏障，令攻擊者難以進行完整連接埠掃描來蒐集目標網絡資料。

使用IPv6 的保安風險
IPv6 雖然比IPv4 標準較爲安全，但同時也帶來新的保安問題，例如：

1. IPv6 支援無狀態位址自動配置(Stateless Address Auto Configuration)，使用IPv6 的電腦可在連接網絡時進行自動配置，取得位址。不過，如果配置不當，便會造成保安漏洞，令攻擊者有機可乘，例如向各IPv6 的電腦分發虛假的網路資訊，令該電腦不能正常運作，導致拒絕服務(denial of service)。

2. 此外，由 IPv4 過渡至IPv6 期間，可能須要使用轉換工具，包括轉換機制及隧道路由器(Tunneling Router)等，讓用戶可以同時使用IPv6 和IPv4網絡。如使用這些轉換工具時沒有周詳地考慮保安問題，攻擊者便有機會藉此進行攻擊。例如，一些防火牆及網絡入侵防禦系統(Intrusion Prevention System，IPS)只能過濾IPv4 的封包，而無法過濾IPv6 的封包。攻擊者可能會利用這個漏洞，使用IPv6 滲入網絡進行攻擊。

一般保安預防措施
在採用IPv6 標準之前，你必須周詳地評估以上的保安風險，作出適當的配置，將風險減低；並爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，安裝防火牆和最新保安修補程式，每周最少全面掃描電腦一次，以及啓動相關軟件的「自動更新」功能。

考考你
1. 下列哪項是IPv6 的保安特性？
A) 互聯網規約保安(IPsec)
B) 大量位址空間使完整掃描連接埠的難度增加
C) IPv6 位址可以跟已簽署的公開密碼匙連結在一起，使仿冒與竊取位址更加困難
D) 以上皆是

2. 採用IPv6 標準之前，必須周詳地評估保安風險，並爲電腦採取下列哪項基本保安措施？
A) 安裝反惡意程式碼軟件如防毒軟件
B) 安裝防火牆和最新保安修補程式
C) 每周最少全面掃描電腦一次，以及啓動相關軟件的「自動更新」功能
D) 以上皆是

46－ 即時通訊的保安威脅

即時通訊(Instant Messaging，IM)是一種電子通訊模式，透過近乎即時傳送和接收網絡訊息的功能進行通訊。隨着即時通訊服務日趨普及，愈來愈多人正享受這些服務帶來的便利。

除了收發網絡訊息外，一些即時通訊服務更可讓用戶與其他人分享網頁連結、相片或其他檔案等。這亦成爲散播病毒和惡性程式碼的另類渠道。

潛在保安威脅

以下是即時通訊服務的主要潛在威脅：

1. 散播惡性程式碼：帶有附件的濫發訊息可透過即時通訊網絡傳送給用戶，這些訊息或其附件可能帶有惡性程式碼，例如電腦病毒，如果使用者不小心開啓這類惡意附件，電腦病毒便有機會透過即時通訊網絡散播給其他用戶。

2. 即時通訊軟件保安漏洞：一如其他應用程式或軟件，即時通訊軟件也有潛在的保安漏洞，攻擊者有機會利用這些保安漏洞對電腦進行攻擊。

3. 敏感資料外泄：即時通訊服務一般都沒有提供加密功能保護傳輸中的訊息，因此，攻擊者可能利用這保安漏洞發動攻擊，例如中間人攻擊，以讀取傳輸中的敏感資料，導致資料外泄。

保安措施

即時通訊服務用戶的一般保安措施包括 ：

1. 在即時通訊客戶端設定不要自動接受所有邀請，避免接收攻擊者傳送來的惡意訊息，亦可避免開啓藏有惡性程式碼的電腦檔案。

2. 開啓從即時通訊服務接收的檔案前，向寄送者查證檔案的真實性並用防毒軟件掃描檔案。

3. 如果即時通訊訊息是由陌生人發出，而又含有網頁連結，千萬不要按下該網頁連結，以免因而感染及傳播電腦病毒。

4. 盡量避免使用即時通訊服務傳送個人或敏感資料，如有必要，也應確保敏感資料已被加密才傳送。

5. 必須在電腦上採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新保安修補程式，每周最少全面掃描電腦一次，及啓動相關軟件的「自動更新」功能。

考考你

1. 下列哪項是即時通訊服務的主要潛在威脅？

A) 散播惡性程式碼
B) 即時通訊軟件保安漏洞
C) 敏感資料外泄
D) 以上全部皆是

2. 下列哪項不是即時通訊服務用戶的一般保安措施？

A) 自動接受所有即時通訊的邀請
B) 避免開啓陌生人寄來的電腦檔案
C) 避免使用即時通訊服務傳送個人或敏感資料
D) 在電腦上採取基本保安措施

47－ 社交網站的保安威脅

社交網站如Facebook、MySpace 及Twitter 等，可讓志同道合的朋友或互不認識的人在網上溝通聯繫並建立社交網絡，分享共同嗜好和興趣。

使用社交網站的保安風險

社交網站爲用戶帶來多元化的網上溝通渠道，例如聊天室、即時通訊、電子郵件、相片及影片分享等，吸引用戶互相分享資訊及多媒體訊息，甚至個人資料。不過，社交網站也同時帶來以下的保安風險:

※ 私隱威脅：用戶或會在社交網站分享大量個人資料，包括個人活動、出生日期、電話號碼等，而這些資料可以輕易從網站取得，心懷不軌的人容易有機可乘，從而侵犯個人私隱。

※ 敏感資料外泄:有些用戶不但分享個人資料，更把工作上的敏感資料上載到社交網站。這些資料一旦外泄，將對用戶不利，亦有損其工作機構的信譽。

※ 惡性程式碼:社交網絡服務通常提供由不同人士編寫的應用程式，爲用戶帶來豐富的娛樂及功能，這些應用程式可能由意圖不軌的攻擊者特別編寫出來，內藏惡性程式碼(Malicious Code)。用戶在不知情下執行這些應用程式，便有機會使其電腦感染電腦病毒，甚至散播給朋友。

※ 社交工程攻擊:社交網絡服務讓用戶建立網絡社羣。心懷不軌的人或會假冒用戶所信賴的朋友，哄騙用戶披露敏感資料，又或者誘使用戶點擊內藏惡性程式碼的連結或開啓含有電腦病毒的檔案，令電腦病毒、木馬等惡性程式碼更容易快速散播。

※ 濫發訊息(Spam):攻擊者可利用社交網站所提供的訊息服務濫發大量訊息，在未經用戶同意下，向他們推銷產品和服務，甚至散播惡性程式碼如電腦病毒。

保安措施

在使用社交網絡服務時，我們必須採取以下的保安措施:

※ 如非必要，切勿公開個人或敏感資料，例如地址、出生日期、機構內部文件、電話號碼、信用卡號碼或個人活動的資料，在分享其他人的資料時，亦應顧及他人的私隱；

※ 應設定一個易記難猜的登入密碼，以減低帳戶被盜用的風險；

※ 應學會如何使用社交網站的私隱設定。網站預設的私隱設定通常容許所有人閱覽你的個人檔案，而你可改變設定爲只准獲授權者閱覽。因爲社交網站的私隱設定可能會更新，所以你須要定期檢查，確保該設定安全及有效；

※ 應審慎考慮允許哪些人跟你聯絡；與網上的陌生人分享時，應考慮適量地分享一般資料，千萬不要與其他人分享敏感資料；

※ 應時刻保持警惕，避免執行社交網站上可疑的應用程式，切勿點擊陌生人所提供的可疑連結。即使瀏覽朋友的網頁，亦要避免點擊網頁所載的可疑連結或圖片，因爲社交網站上的連結、圖片或應用程式都可能含有惡性程式碼；

※ 一些社交網站或會提供濫發訊息過濾或類似黑名單(Blacklist)設定的功能，應考慮使用；

※ 必須在電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新保安修補程式，每周最少全面掃描電腦一次，及啓動相關軟件的「自動更新」功能。

考考你

1. 下列哪項保安風險會在社交網站上出現？

A) 私隱威脅

B) 惡性程式碼

C) 社交工程攻擊

D) 以上皆是

2. 下列哪項是使用社交網站時要採取的保安措施？

A) 公開個人及敏感資料

B) 設定一個易記難猜的登入密碼

C) 使用社交網站預設的私隱設定

D) 點擊陌生人所提供的可疑連結

48－ 對等式網絡(Peer-to-peer (P2P) Network)

什麼是對等式網絡？

對等式網絡是一種非傳統的網絡模式。在對等式網絡上，每部電腦也同時扮演客戶與伺服器的角色。這些電腦不但可以發出要求，同時亦能回應該網絡上其他電腦的要求。對等式網絡通常應用於檔案分享、以IP 爲基礎的網絡電話及網絡電視等用途。

使用對等式網絡的保安風險

使用對等式網絡會面對一定的保安風險，以下是具體的說明：

※ 使用對等式檔案分享軟件時，須設定某一檔案、資料夾或磁碟機爲分享資源。所有儲存在那些地方的資料，包括敏感或個人資料，可能會在用戶不知情下，被他人讀取或在互聯網上公開。但要收回已分享的資料、或尋找曾下載者，是十分困難的。

※ 此外，若某部電腦曾在對等式網絡上分享其便攜式電子裝置上的資料，當插入其他便攜式電子裝置於電腦時，儲存在該裝置內的資料也會同時在用戶不爲意下在網絡上公開。

※ 使用對等式檔案分享軟件下載檔案時，用戶不會知道檔案的可信性。這些檔案可能包含惡性程式碼(Malicious Code)或其他非法的內容，下載並安裝後，用戶的電腦便會被入侵。

※ 如同其他的軟件，對等式軟件亦存在保安漏洞。入侵者可能利用保安漏洞攻擊用戶電腦。

一般保安預防措施

要防止對等式網絡所帶來的風險，機構或個別用戶也要採取適當的保安預防措施。例如：

機構方面

※ 若在日常營運上沒有需要，應禁止員工下載及安裝對等式軟件。如在員工的工作電腦上發現對等式軟件，應儘快移除。

※ 機構須考慮使用入侵偵測系統(Intrusion Detection System，IDS)監控網絡傳輸活動，並即時封鎖任何未經授權的對等式網絡傳輸。

個別用戶方面
※ 不應在對等式網絡上分享任何敏感或個人的資料。
※ 不要下載含有淫褻或非法內容的檔案或軟件，包括盜版軟件。
※ 不應把對等式軟件設定爲開機時自動啓動模式。
※ 若必須下載對等式網絡上的檔案，應在下載完成後立即關閉該軟件。

另外，你必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，及啓動相關軟件「自動更新」功能。

考考你
1. 對等式網絡是否指每部在網絡上的電腦，同時扮演著一個客戶與一個伺服器的角色？

2. 使用對等式網絡要面對甚麼保安風險？
I) 散佈惡性程式碼
II) 收到濫發電郵
III)泄漏敏感或個人的資料
A) I & II
B) I & III
C) II & III

49－ 電子交易的保安考慮(I)

什麼是電子交易?
電子交易是指利用電子系統進行交易活動，隨著互聯網日漸普及，相關的電子交易服務，如網上購物或網上銀行，已經甚爲普遍。

現時很多網站都會提供網上購物服務，用戶只需要揀選想購買的商品，按下「遞交訂單」按鈕，便能透過不同的網上購物付款方案付款，常見方案包括信用卡或付款集合人(Payment Aggregator) 等。付款成功後，網站便會根據訂單的相關細則運送商品給用戶。

網上銀行是另一種常見的電子交易服務，用戶登入自己的網上銀行賬戶，便可管理自己的資產，以及進行轉賬、繳付賬單或買賣股票等。

電子交易的保安風險
電子交易帶來方便快捷的服務，但同時也帶來保安風險。進行電子交易服務時，一般都需要用戶提交使用者名稱和密碼，以及其他敏感資料，如信用卡號碼或用戶姓名，電子交易亦因此成爲了仿冒詐騙 (Phishing) 攻擊的目標。

攻擊者會利用仿冒電子郵件或欺詐網站，誤導毫無戒心的網絡用戶，騙取個人資料。

如果在交易前，用戶沒有確認網站的真確性及細閱其交易細則，或者沒有進行適當的身分認證及將傳輸的資料加密，敏感資料就有機會外泄，被入侵者用作非法用途，如身分盜用 (Identity Theft) 等。

考考你

1.下列哪項是用戶要留意的仿冒詐騙工具？

A) 仿冒電子郵件

B) 欺詐網站

C) 以上皆是

2.下列哪項措施可以在進行電子交易時減低敏感資料外泄的機會？

A) 確認網站的真確性

B) 細閱其交易細則

C) 進行適當的身分認證

D) 以上皆是

50－ 電子交易的保安考慮(II)

一般保安預防措施

進行電子交易服務時，有什麼地方要注意呢？

機構方面

※ 如果網站需要用戶輸入敏感資料，網站應提供伺服器電子證書，讓用戶核實網站的真確性。用戶應檢查電子證書的內容，例如證書簽發機關及有效日期等。

※ 機構提供網上購物服務時，可考慮採用「持卡人身分驗證」服務。用戶在網上購物時，除了輸入信用卡號碼外，還必須向發卡機構提供一組預先登記的個人密碼，作爲核實持卡人身分之用，有了這雙重保障，用戶身分被盜用的機會便可減低。

※ 機構提供網上銀行服務時，盡可能使用雙重認證 (Two-Factor Authentication) 。雙重認證是指採用兩種不同性質的因素以核實用戶身分。例如用戶登入銀行賬戶或確認交易時，除了輸入使用者名稱和密碼外，還必須利用公開密碼匙基礎建設(PKI)機制中的數碼證書 (digital certificate)，作爲額外核證之用。另外一個例子是以手提電話接收或使用保安編碼器(security device)所產生的限用一次密碼(one-time password)，這組密碼只能使用一次，並會在短時間內失效，這樣入侵者便較難盜取用戶身分。

個人方面

※ 在使用網吧或其他公共上網設施時，不要進行網上交易活動，或使用網上銀行服務。

※ 使用電子交易服務前，應先關閉所有瀏覽器視窗，以免其他網站非法取得你的個人資料。在完成網上交易後，應登出服務。

※ 提供個人或賬戶資料時，應保持警惕。銀行及金融機構一般不會透過電郵要求客戶提供個人或賬戶資料。如有疑問，應向相關機構查詢。

※ 不要按可疑電郵內的連結或從搜尋器搜尋到的銀行或其他金融機構網址，應以人手直接輸入URL 網址或使用之前已加入書簽的連結。
※ 定期登入網上戶口，檢查賬戶狀況、交易紀錄及上次登入日期，查看是否有可疑交易活動。

另外，必須爲電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新保安修補程式，每周最少全面掃描電腦一次，及啓動相關軟件「自動更新」功能。

考考你
1. 下列哪項不是雙重認證對電子交易的功用？
A) 核實用戶身分
B) 減低用戶身分被盜用的機會
C) 作爲買賣雙方辨認交易貨幣之用
D) 作爲額外核證之用

2. 下列哪項是使用電子交易服務時要採取的保安措施？
A) 在電郵內提供個人或賬戶資料
B) 在公共上網設施進行網上交易活動
C) 完成網上交易後登出服務
D) 點擊可疑電郵內的連結

51－ 開放源碼軟件保安

開放源碼軟件是指可供任何人使用，甚至改寫源碼並重新推出作其他用途的軟件。

開放源碼軟件通常附帶其軟件特許使用權証(open source licence)或一些使用條款。在選用開放源碼軟件時，除了考慮軟件的功能外，還要詳細閱讀其軟件特許使用權証和使用條款上的限制。
有些機構，例如開放源碼促進會(Open Source Initiative)，已就開放源碼軟件的軟件特許使用權証進行檢討。機構會按既定標準審視這些軟件特許使用權証是否符合既定要求。

開放源碼軟件的保安威脅
開放源碼軟件的源碼是開放給大眾，因此攻擊者也可能利用源碼的保安漏洞進行攻擊。如同使用封閉式源碼軟件，用戶電腦亦可能透過以下途徑受到攻擊者的襲擊：
※ 從可疑的網站或連結下載及安裝包含惡性程式碼的軟件；
※ 沒有替軟件安裝保安修補程式，令攻擊者有機可乘，藉着已知的保安漏洞，入侵用戶電腦。

開放源碼軟件保安的最佳作業實務
以下是開放源碼軟件保安的一些最佳作業實務：
(一) 制定及定期更新一份已安裝軟件的清單，該清單應詳細記錄軟件的來源網站、版本和雜湊值(hash value)，例如雜湊函數算法(secure hash algorithm，SHA)，以方便核對源碼的完整性。
(二) 定期執行修補程式管理流程，如檢查開放源碼軟件的更新和錯誤修正，減少開放源碼軟件的保安漏洞。
(三) 在安裝開放源碼軟件後，應盡快更改所有預設的保安設定，並關閉不需要的服務功能。
(四) 以編碼分析器(code analysers)或審計工具(auditing tools)來測試和掃描源碼。

機構必須考慮以下幾方面：
※ 爲員工提供適當訓練，以支援和維護開放源碼產品。
※ 制定妥善記錄的保安政策，並嚴格執行，例如員工必須清楚記錄所有作業實務和配置程序，避免因職務調動或離職而引起問題。
※ 應用開放源碼軟件前，必須先進行保安風險評估 (security risk assessment)，並在應用後定期覆檢。

考考你
1. 在制定已安裝軟件的清單時，下列哪項應該詳細記錄下來？
A) 軟件版本
B) 軟件的來源網站
C) 軟件的雜湊值
D) 以上皆是

2. 編碼分析器(code analysers)或審計工具(auditing tools) 可以找出源碼的保安漏洞？

52－ 無線網絡設置保安

無線網絡(Wi-Fi)一般是指用戶利用無線電腦裝置，在無線網絡覆蓋範圍之內，透過無線網絡路由器連接至互聯網。如果沒有妥善的設置，無線網絡可能會引起資訊保安事故，有機會導致網絡被入侵或資料被竊取。

無線網絡的保安設置
無線網絡路由器(router)或無線接駁點(wireless access point)是無線網絡中的重要硬件之一，由於無線網絡路由器通常已包含無線接駁點的所有功能，以下會以無線網絡路由器作爲例子繼續說明。在出廠時一般都預設了服務設定識別碼(Service Set Identifier，SSID)、用戶名稱、密碼等內容，而通常同一製造商出產的無線網絡路由器，預設的內容都是一樣的。

更改預設內容
無線網絡路由器會使用SSID 來稱呼該網絡，而該預設的SSID 名稱有可能在互聯網上找到。

因此，攻擊者便可藉這個漏洞進一步收集資料，例如預設的用戶名稱及密碼，繼而進行攻擊。因此，在設置無線網絡路由器時，應第一時間更改預設的SSID、用戶名稱及密碼，以免被攻擊者有機可乘。

使用連線加密

大部分無線網絡路由器都具備加密功能，應選取合適的加密技術及相關設定，以確保在無線網絡上傳送的訊息不會輕易外泄。

啓用MAC 地址過濾功能

每個無線電腦裝置在出廠時一般擁有獨一無二的MAC 地址。無線網絡管理員可設置無線網絡路由器，啓用 MAC 地址過濾功能，只允許擁有指定MAC 地址的無線電腦裝置連接該無線網絡。這樣，攻擊者便不能輕易利用其他擁有不同MAC地址的電腦，連接該無線網絡。

其他保安措施

此外，還須注意其他無線網絡設置的保安措施，例如:

※ 每部無線電腦裝置都應安裝及啓動防火牆，而無線網絡路由器的內置防火牆功能亦應同時啓動。

※ 把 SSID 廣播功能關閉，減低被攻擊的可能性。

※ 在無須使用無線網絡時，或網絡受攻擊時，應關閉無線網絡路由器。

※ 應盡量將無線網絡路由器安裝在使用範圍的中心位置，不要靠近窗戶，減低無線訊號發放到公共地方的可能性。

考考你

1. 下列哪項無線網絡路由器保安設定能減低無線網絡被入侵或資料被竊取風險？

A) 啓用加密功能
B) 啓用MAC 地址過濾功能
C) 關閉SSID 廣播功能
D) 以上全部皆是

2. 無線網絡路由器放置於靠近窗戶的位置，是否能減低無線訊號發放到公共地方的可能性？