第 7 課 網上防騙及保安

隨著越來越多老友記於日常生活中使用數碼科技，老友記遇到網上騙案的機會亦相應增加。老友記必須提高警覺，才能避免成為網上騙案的受害者。

網上騙案種類

電郵騙案：有時我們會收到一些來歷不明的電郵，聲稱你中了大獎又或者有一筆巨款等你去領取，誘使你繳交手續費或保證金，事後當然領取不了這些不存在的「獎金」。

網上購物騙案：於網上購物後久久未能收貨，賣家又失蹤，無法聯絡。

社交媒體騙案：騙徒在社交平台結識受害人，待雙方熟絡之後，就會以各種不同藉口向受害人騙取金錢。又或騙徒以非法途徑取得社交媒體帳戶的登入名稱及密碼，然後冒充他人聯絡通訊錄上的朋友，借故要求對方代為購買點數卡或充值卡。騙徒得手之後就會失去聯絡。

網上銀行騙案：以各種方式非法登入受害人的網上銀行帳戶，然後轉走存款。例如冒稱某些機構人員，要求受害人交出網上銀行戶口密碼，或假冒銀行向受害人發出偽冒電郵，誘騙受害人開啟電郵內連結，在偽冒網站中輸入網上銀行的登入資料。

其他常見的科技罪案

勒索軟件攻擊：以電郵向受害人傳送勒索軟件，當受害人一不小心開啟電郵內的附件後，電腦內的檔案就會被加密，騙徒便藉此要求受害人繳付贖金以解密檔案。

虛假消息：刻意讓一些虛假消息在網上流傳，不但影響社會秩序，亦可能引起市民恐慌。

「防騙錦囊」

安全小貼士	智能裝置的安全措施
● 網上購物時，要注意以下幾點： ✓ 盡可能光顧有信譽的商戶 ✓ 即使網店是由可信賴的人介紹，亦要事先做好資料搜集，評估賣家是否可靠 ✓ 先購買小額或少量貨品，在收到貨品並認為賣家值得信任之後，才考慮再次購買 ✓ 盡量要求賣家面對面交易或貨到付款 ✓ 記下賣家資料（如帳戶號碼），並要求賣家提供容易辨識身份的收款銀行戶口 ✓ 臨近出貨日期前可以向賣家查詢出貨情況。如果發現賣家失去聯絡，盡快嘗試用其他方法核實賣家是否有可疑 ● 不要打開不明來歷的訊息或電郵，並且不要隨便打開電郵內的連結和附件 ● 如果電腦檔案被勒索軟件加密，不應繳付贖金，而應該立即向警方求助 ● 不要轉發未經證實的消息	● 建立安全的鎖機密碼及帳戶密碼 ● 避免向第三者透露任何密碼 ● 不同帳戶應該使用不同密碼 ● 如懷疑自己的密碼已被泄露，應立即更改密碼 ● 只從官方應用程式商店安裝應用程式 ● 安裝及使用軟件／應用程式時，只賦予該軟件／應用程式在運行中必須使用的權限 ● 定期更新智能裝置上的作業系統及流動應用程式 ● 萬一遺失智能裝置，應盡快使用遙距鎖機或遙距清除裝置上所有資料

雙重認證

「雙重認證」是指系統同時利用以下三種驗證方法的*其中兩種*，去確定登入人士的身份。

What you know（你所知道的資料）：只有你知道，而其他人不知道的資訊，例如密碼。

What you have（你所擁有的憑證）：只有你手上持有，而其他人並未擁有的憑證，例如網上銀行提供的保安編碼器。

What you are（你本人的特徵）：簡單而言就是以你的生物特徵作為認證，例如面容、指紋、聲紋、靜脈、視網膜等。

建議老友記在支援「雙重認證」的網上帳戶中啟用「雙重認證」功能。啟用「雙重認證」後，登入時除了需要輸入帳戶名稱及密碼外，還要使用保安編碼器提供的編碼、面容或指紋等進行第二重驗證後才能成功登入。