

# TELUS Wise®

## 數碼安全及隱私保護知識



TELUS Wise 是一項免費教育計劃，該計劃的宗旨是保障加國民眾的數碼安全。以下知識可幫助您和您的家人的安全。



### 網絡安全

- 1. 自我保護：** 使用防病毒、防間諜軟件和防火牆安全方案，並記得定期備份資料數據。
- 2. 確保軟件、操作系統及瀏覽器為最新版本，** 以確保始終保護您的系統免受最新威脅的侵害。
- 3. 設置複雜密碼，** 並經常更改它們以增強安全性。
- 4. 仔細檢查您的電子郵件：** 可疑的附件/鏈接、個人信息請求、拼寫錯誤和語法錯誤，都有助您發現可能有害的電子郵件。



### 智能手機及平板電腦安全

- 1. 設立手機密碼：** 為手機設置安全密碼鎖，在其一段不使用時間後自動上鎖。不要忘記定期設置及更改密碼。
- 2. 鎖定、追蹤、刪除等應用程式：** 當您的手機被盜或丟失時，視乎您的操作系統而定，您可使用相應的應用程式鎖定、追蹤或遠程刪除手機上的所有資料。（在iPhone上，該應用程式名叫“尋找我的手機”，而在Blackberry手機上，則叫Blackberry Protect Android系統上，具體名稱因製造商的不同而異）。此外，在舊機換購或回收時，記得徹底刪除您手機上的資料。
- 3. 定期更新您的系統，** 以獲得最新的安全威脅防護。
- 4. 地理位置設定：** 僅向需要知道您所在位置的應用授予位置訪問權限，例如GPS或地圖。應用社交媒體和許多其他應用程式無需位置信息設定亦可運行。
- 5. 請勿打開來自未知來源的**附件及下載應用程式前，應了解清楚詳情，以免安裝了惡意軟件到您的設備上。
- 6. 謹慎使用免費Wi-Fi：** 黑客可以輕鬆獲取您的個人資料；如果您在公共場所使用免費Wi-Fi，請僅限瀏覽網頁。永遠不要透過免費Wi-Fi網絡分享私人或財務信息。
- 7. 注意藍牙連線風險：** 黑客也可能透過訪問藍牙設備上的信息或與進行未經授權的連接。僅啟用與可信任設備的連接和/或在不需要使用的時候，關閉藍牙。



### 社交媒體安全

- 1. 密切關注權限和隱私設定：**
  - **權限設定**可以讓您控制分享和不分享您的資料（例如，聯繫人列表、照片和您的個人資料信息）。
  - **隱私設定**控制誰可以及不可以查看您的個人資料和帖子。
- 2. 設定Google提示：** 在google.com/alerts 為您的姓名設定Google提示。每當您的姓名上線時，即會通過電子郵件通知您。
- 3. 限制您分享的內容：** 分享過多的信息，例如您的出生日期、地址和假期詳情可能會增加您的風險。
- 4. 建立聯繫方式前請三思：** 只和當面認識過的人建立聯繫。
- 5. 點擊網絡鏈接要小心：** 不要點擊可疑的鏈接或好得不太真實的優惠。
- 6. 關閉地理標記：** 大多數智能手機拍攝的照片都包括有地理標記（拍攝圖像的確切位置詳細信息）。在網絡上分享照片時，請關閉此功能，以增強隱私保護。
- 7. 不要忘記註銷帳戶：** 在不使用時讓社交媒體帳戶、應用程式或遊戲處在打開狀態時，會使您易受到安全和隱私威脅。
- 8. 保持數碼帳戶清潔：** 在日曆中設置提醒，每隔三至六個月檢查社交媒體帳戶和應用程式上的隱私和權限設置。更改密碼、審核和清理您的“朋友”列表，並停用您不再使用的帳戶。



## 網上購物安全

1. **驗證賣家的聲譽**：在網站上查找隱私聲明、真實地址、電話號碼和退貨政策，並查看其他客戶的正面評價。
2. **確認安全性**：查找鎖定符號和在地址欄中“https”的“s”

 Secure | <https://wise.telus.com/en>

3. **保護您的資料**：不要在公共電腦上或通過共享Wi-Fi網絡進行網購，並應始終拒絕任何保存您的信用卡信息的選項。



## 分心駕駛

讓我們達成共識，就是分心駕駛是不可接受的。

保持雙手放在方向盤上，眼觀前路，並遵守以下提示：

1. 將手機放到視線以外的地方，並不要去想著看手機（例如：車廂的儲物箱）
2. 將手機調至靜音或關機
3. 您的乘客替您暫時保管手機
4. 在開車前檢查短訊及設定好GPS導航
5. 必須使用手機，則須安全將車停在路邊



## 物聯網安全

物聯網是指智能或透過互聯網可彼此連接的設備系統，例如家庭安防系統、嬰兒監視器、智能手錶等等。這些設備徹底改變了我們的生活方式，但它們會收集和傳輸數據，因此應謹慎留意以下問題：

1. 了解有哪些數據已被搜集，以及如何被使用。
2. 管理隱私設定，這樣您的數據只會被分享給您想要分享的及願意分享的一方。
3. 在不使用物聯網設備時，應及時關閉它（特別是帶有攝像頭/麥克風的設備）。
4. 物聯網設備單獨使用“訪客”專用網絡，這樣可確保您的個人網絡不會被黑客利用。

您知道嗎？42%的年輕人都遭受過網絡欺凌。  
它有很多形式表現，而且不僅對青少年造成影響。

遭遇網絡欺凌，可以遵循以下四個步驟處理：

1. **停止參與**，並立即離開該網絡空間；爭論會令局勢變得更嚴重。
2. 如果可以的話，**封鎖所有短訊**，和/或通過社交媒體平台舉報/封鎖此人。
3. **記錄相關短訊信息**以便於日後調查；將屏幕截圖以保存證據。
4. **告知他人此事並商討行動方案**。如果您無法解決問題和/或感到受到威脅，您應聯繫當地執法機構。

瀏覽 [telus.com/riseabove](https://www.telus.com/riseabove) 獲取更多相關資訊。

更多詳情請瀏覽 [telus.com/wise](https://www.telus.com/wise) 或發郵件至 [wise@telus.com](mailto:wise@telus.com) 預約講座。  
歡迎參加我們的線上討論 [#TELUSWise](https://www.telus.com/wise)



獲加拿大警察總長協會大力支持，  
TELUS Wise項目已吸引超過300萬  
加拿大人的參與。



簡易精彩 啟迪未來®