

Skype 安全資源中心

安全性部分

保持電腦安全可靠是電腦使用者和軟體製造商(如 Skype)共同肩負的責任。Skype 重視安全性，並考慮到目前和將來的安全威脅，採取了許多步驟來開發我們的軟體。

Skype 的主要安全性領域分為以下方面：

Skype 的數位身份證明和加密

Skype 的主要目標之一是防止我們的使用者受到未授權的竊聽。出於這一考慮，我們希望杜絕行騙者在透過電子郵件行騙時慣用的假冒手段，他們藉由這些手段來騙使用者提供有價值的個人資訊。

為達到上述目標，Skype 向每名 Skype 使用者頒發了一個「數位證書」，任何 Skype 使用者均可出示該證書，以便確定發起或接受 Skype 通話或聊天的人員的身份。這些數位證書形成了 Skype 線上目錄的核心，它可允許使用者找到網際網路上的其他使用者，而無需線上人員的中央清單。

什麼是數位證書？

數位證書是一種電子證書，可用於確認 Skype 使用者的身份，無論該使用者位於何處。像實體身份證明文件（例如駕照）一樣，數位證書必須擁有特定內容，以使用作一種識別手段。具體而言，它必須：

- * 指定被識別的特定帳戶；
- * 由一個可隨時撤銷證書的機構頒發；
- * 難以假冒；
- * 含有頒發機構的連署簽名，在本例中為 Skype。

認證

由於 Skype 使用者均擁有數位證書，因此任何 Skype 使用者都可以確認任何其他 Skype 使用者的身份。這一過程稱為認證：將各方的真實身份提供給對方。

認證是確保安全通訊一個關鍵步驟。想像一下，若您正和一名自稱是業務夥伴的人聊天，但他實

實際上是一名冒名頂替者，那會是什麼情形？聊天內容可能已盡量高度加密，但私有資訊洩露的情況仍有可能發生。

加密

犯罪分子和駭客可從多種位置對網際網路之類的通訊網路進行監控。從安全角度看，這是電子郵件和許多網際網路聊天程式被認為不安全的一個原因。換言之，由於未知人員有太多方式監控使用者的通訊，因此使用者必須採取積極的措施來避免自己受到此類入侵。

加密是使用數學原理給訊息編碼的過程，只有預期收件人才能讀取加密的訊息。數個世紀以來，各種加密方法層出不窮，但它們都類似於一個上鎖的箱子和鑰匙：一旦秘密訊息被放入有鎖的箱子並用鑰匙上鎖，只有擁有相同鑰匙的人才能再次讀取它。

Skype 使用基於標準的知名加密算法，以防止 Skype 使用者的通訊內容落入駭客和犯罪分子之手。透過這種方式，Skype 可確保使用者的隱私以及資料在使用者之間傳送時的完整性。

獨立安全性評估

這份 Skype 加密評估（PGP 簽名檔）對 Skype 產品採用的安全架構做了詳盡的分析。Skype 保護使用者免受各式各樣的潛在攻擊，例如假冒身份、竊聽、中間人攻擊以及修改傳輸中的數據。

該報告說明了整個 Skype 基礎設施所採用的一般保護機制，以及界定了 Skype 運作架構內所有設計的總體安全政策。

防火牆與 Skype

Skype 是一個同儕通訊應用程式，表示它依賴於能夠直接透過網際網路將訊息傳送至其他使用者的電腦。同樣，若使用者能夠暢通無阻地透過網際網路在彼此之間直接通訊，則 Skype 的運作效率最高。

防火牆是設定用來防止電腦網路進行外部存取的裝置，從而攔截網際網路上潛在惡意使用者的攻擊。使用者網路上存在的防火牆常常會讓使用者無法直接收到來自其他使用者的通訊，這可能會降低語音通話的品質。

然而，即使位於防火牆後面，Skype 也能運作得很好。這是因為當 Skype 在位於防火牆後面的網路上執行時，它會「向外」連接至網際網路。Skype 不會以任何方式修改網路上的防火牆或干擾其使用。儘管有時透過允許來自網際網路的輸入連線可提高 Skype 通話的品質，但並不需要設定特殊的防火牆規則或例外情況。

一般電腦安全

要確保您的電腦安全可靠，最重要的步驟是遵守良好的一般安全實踐：

1. 安裝和使用防毒程式，以避免您的電腦受到線上威脅，無論它們以何種方式傳送至您的電腦。
2. 安裝更新或修補程式，例如使用 **Windows Update** 服務，使您電腦的作業系統保持最新。
3. 不要打開檔案附件，特別是來源不可靠的郵件。
4. 安裝和使用防火牆程式。
5. 對重要檔案和資料夾進行備份。
6. 使用複雜的、難以猜到的密碼。
7. 在下載和安裝程式時請小心。

我們建議使用者閱讀並遵守 CERT® 協調中心提倡的 [Safe Computing Tips \(電腦安全使用技巧\)](#)。