# 提升檔案的安全性

以下提供一些定義，讓您了解對手的危險性：

**病毒**   撰寫軟體 (或程式碼) 的明顯意圖是進行自我複製。病毒會自動附加在另一個檔案或程式中，在電腦之間散佈。

**蠕蟲**    透過網路連線傳送至其他系統，單獨地進行自我複製的軟體。

**木馬病毒**    看起來有用或無害的軟體，但其中包含隱藏程式碼，用來攻擊或損毀執行軟體的系統。

**間接軟體**    顯示廣告 (例如彈出式廣告)、收集使用者資訊，或變更使用者電腦設定的軟體，通常都沒有經過使用者的同意。

**網路釣魚**    透過電子郵件擷取使用者個人資訊 (例如銀行或信用卡詳細資料) 的方法。

第一要務：保護您的電腦

您可能不知道電腦已經成為鎖定的目標。這不是您個人的原因，所有的電腦都是目標。有些人會嘗試破壞您的電腦或存取其中的資料，設法從中牟利，或只是純粹破壞。您必須認清危險性，並學習如何保護電腦的安全。

認清敵人：這個課程將為您介紹各種電腦風險，並提供避免風險的建議。

安全性威脅

您可能已經從新聞媒體聽過這些名詞：病毒、蠕蟲、木馬病毒、網路釣魚及間諜軟體。如果要採取提升電腦安全性的動作，您必須先知道一些基本資訊，了解電腦所面臨的危險性。

大部分的安全性威脅都包含**惡意軟體** (或程式碼)，會在您不知情的情況下，在電腦上執行。它可能隱藏在另一個檔案或程式中，或是在背景中自動執行。大部分的惡意軟體都設計成自我複製，並感染其他的檔案或電腦。感染電腦的一個途徑是取得您所有的連絡人地址，並傳送包含惡意軟體的「已感染」電子郵件，讓它看起來像是您寄出的。

惡意程式碼的特性和破壞性決定了它對電腦所造成的影響，它可能只會造成一些小困擾，也可能會刪除檔案或程式，破壞您的電腦。