誰是您網路安全的 最大敵人？

1. 駭客（Hackers）

這類型的電腦狂熱份子，常以竊取他人電腦權限為樂！

許多駭客會在破解他人電腦後留下「證據」（某些玩笑性的小程式或訊息），有些駭客則是更具惡意的破壞者，稱為「crackers」；他們會造成整個網路癱瘓、竊取或破壞機密資料，損毀網頁並中斷網路交易進行。

但是，並非所有駭客都是天才。即使他們不知道程式如何運作或造成的後果為何，都可藉由網路上許多簡單的駭客工具程式來進行破壞。

2000 年，85% 的企業與政府機構曾遭受駭客攻擊。

2. 警覺性不足的員工

當員工專注於工作時，很可能忽略網路安全標準程序，如所使用的密碼很容易可猜到，或可以工具軟體破解。

其次，員工可能不經意造成電腦病毒感染與傳播，例如使用受感染磁片或從網路上下載受感染的程式，使得病毒進入系統。

無論是電腦新手或專家，員工都有可能犯下不當地安裝防毒軟體或忽略關於安全威脅警告的錯誤。因此，企業也必須防範人為錯誤。

3. 心懷不滿的員工

相較於無心犯錯，心懷憤恨或報復心態員工所造成的傷害才更需要擔心；通常這些人可能曾受到懲戒、革職或解雇，讓公司網路遭受病毒侵入，或有意刪除重要檔案。

這些人員是非常危險，因為他們很可能熟悉網路、檔案文件中資訊的價值、重要資訊存放位置或相關保護措施。

企業中有 49% 的安全漏洞是由員工造成。

4. 窺探者

無論員工對公司是否滿意，他們可能心存好奇或惡作劇心態。而「窺探者」是指參與企業間諜工作的員工，他們在未經許可的情況下取得公司機密，並交給競爭對手，而這些資訊可能包括公司財務狀況、同事之間電子情書，或薪資。

在這些行為中，雖然部分不會構成重大傷害，但若是取得財務、醫療或人力資源等資料的行為，就會造成嚴重後果，並藉此破壞企業信譽，增加公司成本。