資訊保安要認真

第一堂 介紹資訊安全威脅

視像文字稿

介紹資訊安全威脅

在這個單元裡面，我們會介紹資訊安全的威脅，包括資訊安全威脅的基本概念，一些經常聽到的名詞，例如，黑客、電腦病毒和木馬程式等，之後會介紹常見的網絡威脅。

黑客

首先，我們會介紹什麼是黑客。在主流社會一般都將黑客視作電腦罪犯。其實，這一個名詞原本並沒有電腦罪犯的意思，也因為媒體和影視界通常描述他們進行違法行為，所以我們都會認為黑客只從事犯罪活動。其實，黑客主要指擁有電腦技術水平高超的人士，他們除了精通編程之外，也精通系統操作和網絡技術，還有一些對硬體裝置進行創新工程的人士，都被稱為黑客。而部分從事罪犯活動的黑客，他們會開發一些惡意程式，對個人電腦、伺服器、數碼裝置和網絡等，造成損害或不預期的影響。

惡意程式

惡意程式有不同的種類，例如電腦病毒、特洛伊木馬程式、間諜程式、廣告程式和勒索程式等。接著我們會逐一介紹以上的惡意程式。

電腦病毒

電腦病毒是一種在人為或非人為的情況下產生的、而用戶不知情或未經批准的情況下，能夠自我複製或運行的電腦程式。電腦病毒會對電腦造成不同的傷害，例如降低電腦效能、破壞電腦內的檔案、影響程式運作甚至導致電腦不能啟動。電腦病毒主要通過互聯網傳播，他們會隱藏在電郵的附件、網站或網絡上可供下載的程式和檔案之中。

惡意程式 — 特洛伊木馬程式

一般簡稱為木馬程式，在電腦領域中指的是一種後門程式，是黑客用來盜取其他

用戶的個人資料，甚至遠程控制對方的電腦而製作的程式，然後黑客會通過各種的手段去傳播，或騙取目標使用者去執行這些程式，以達到盜取密碼或數據資料的目的，和電腦病毒很相似，但木馬程式通常不會自我複製，令使用者很難發現它的存在。

惡意程式 — 間諜程式

間諜程式是一種經過或未經過你同意安裝在電腦上面的程式，目的是蒐集關於使用者電腦或瀏覽習慣的資訊，在使用者不知情下蒐集你的操作資訊，之後會把這些資料傳送給黑客。間諜程式通常會在你安裝免費軟件或應用程式的時候，靜悄悄地同時安裝在你的電腦裡面。

惡意程式 — 廣告程式

廣告程式是一個含有廣告的電腦程式，在執行程式的時候顯示廣告，雖然大部分廣告程式對電腦沒有造成傷害，但是仍可以通過彈出式視窗在電腦螢幕上面顯示廣告，對使用者造成滋擾，亦有一些公司利用廣告程式來進行推銷。

惡意程式 — 勒索程式

勒索程式與其他電腦病毒最大的分別是手法和中毒的方式。勒索程式一般會將裝置加密，使受害者無法控制電腦和取回裝置內的檔案。黑客會要求受害者繳付贖金，才有可能取回電腦的控制權或被上鎖的檔案。勒索程式一般通過木馬程式和電子郵件的附件去傳播，有些亦會通過網絡系統的漏洞，在電腦網絡之間傳播。

其他威脅

除了剛剛介紹的惡意程式外，亦有很多其他類型的威脅，例如一些牽涉人為錯誤，例如網絡釣魚、社交工程攻擊、混淆網址、手機遺失後被盜用，和使用不安全的公共無線網絡等的威脅。

其他威脅 — 社交工程攻擊

社交工程攻擊是利用人性的弱點，應用溝通和欺騙技巧，以獲取帳號、密碼、身份證號碼、或其他敏感的資料，突破系統資訊的安全防護，進行非法存取和破壞行為等。

其他威脅 — 網絡釣魚

網絡釣魚一般是通過電子郵件或即時通訊的方式進行，引導用戶到黑客所建立的假冒網站，而網站的網址和介面外觀，會與真正網站很相似，誘騙用戶輸入個人資料，從而偷取個人資料作不法用途。

其他威脅 — 混淆網址

混淆網址是模仿網站的欺騙性網址，這是為了令用戶瀏覽欺騙性的網站的時候，很難發現並非原本的網站。就如我們顯示的事例來說，會將原始網站其中的英文字母「o」變成數目字「0」，令使用者不察覺去了另一個網站。

其他威脅 — 手機因遺失被盜用

遺失手機都是其中一個威脅。當你遺失手機後，而你的手機又沒有設定密碼，就很容易洩漏手機內的資料，例如相片、聯絡人資料、甚至銀行戶口和信用卡資料等。如果使用者有設定手機保安，例如密碼和生物認證等功能，即使遺失手機，也能阻止不法之徒輕易取得手機內的資料。

其他威脅 — 無線網絡威脅

使用不安全的公共無線網絡。當我們連接上不安全的無線網絡的時候，我們經無線網絡傳送的訊息有可能會被截取，又或將流動裝置連接到黑客所裝設的無線網絡，而無線網絡亦可能已經被黑客控制，有可能被連結到有惡意程式的網站，導致帳戶個人資料外洩或流動裝置被惡意程式感染等。

關於介紹資訊安全威脅的單元就來到這裡，下集再見。

本教材由屯輝長者學苑提供內容及製作。