資訊保安動畫 -中間人攻擊（旁白）

中間人攻擊

中間人攻擊(Man-in-the-Middle Attack)，一般是指攻擊者在訊息傳送時，於發送者和接收者之間，暗中讀取、插入及更改訊息的網上攻擊。

入侵途徑

如果發送者在傳送訊息時，沒有將訊息加密(Encryption)，又沒有數碼簽署(Digital Signature)，攻擊者便可利用網絡上的保安漏洞，中途攔截及改變發送者的訊息，再傳回接收者。由於網絡傳輸仍能正常運作，沒有斷線，發送者和接收者都難以察覺傳送的數據，已被攻擊者竊取、攔截或竄改。這種攻擊，一般毋需在用戶電腦上裝上惡性程式碼(Malicious Code)，如電腦病毒或特洛依木馬(Trojan Horse)，也不會在用戶電腦上留下任何紀錄，因此難以被反惡性程式碼軟件(Anti-Malicious Code Software)如防毒軟件發現。

潛在威脅

受到中間人攻擊，你會面對甚麼潛在威脅？

若電腦用戶進行沒有加密的網上交易，中間人便可從傳送的訊息中讀取用戶的銀行帳號及密碼，登入帳戶，偷取金錢，或進行非法交易，令用戶蒙受財務損失。

如入侵者能竊取機構系統登入帳戶及密碼，便有機會盜取機構內部的敏感資料，如客戶個人資料，引致資料外泄。

一般保安預防措施

為了有效防範中間人攻擊，你必須做好保安預防措施。

機構方面：

- 採用加密連線，例如 HTTPS、SSH、SFTP 等等，把網絡的傳輸內容加密。即使入侵者可中途攔截，也不能閱讀或變更資料。
- 使用相互認證(Mutual authentication)，由於用戶的電腦必須通過伺服器(Server)認證，而伺服器亦要通過用戶認證，因此可助阻隔中間人攻擊。

個人方面：

- 設定和啓動 Wi-Fi 通訊的加密功能，如 WPA 以 AES 加密。
- 在使用網吧或其他公共上網設施時，不要進行網上交易活動，或使用網上銀行。

除將訊息加密、使用數碼簽署及採取上述的保安預防措施外，其他各種相關的資

訊保安措施，都不可以忽視。

考考你

請選擇正確的答案。

1. 一般的中間人攻擊會不會在用戶電腦上留下任何紀錄？

A) 會(正確答案)

B) 不會

2. 哪項保安措施有助預防中間人的攻擊？

I) 啟動 Wi-Fi 通訊加密功能

II) 使用相互認證

III)在公眾地方用網上銀行

A) I & II(正確答案)

B) I & III

C) II & III

想知道更多有關資訊保安的資料，請瀏覽「資訊安全網」：

http://www.infosec.gov.hk