

如何防止駭客入侵?資訊安全小秘訣在這裡

1、如何管密碼。創造幾個複雜的密碼片段，加在一起使用，例如，你有 4 段不同的密碼，上甲網站時，你用的是 A 密碼加 B 密碼，上乙網站時，則用 B 密碼加 C 密碼，這樣遠比萬用密碼安全，也簡化記密碼的負擔。

2、把公司和私人郵件信箱分開。很多人為了方便，把公用郵件和私人郵件都寄到同一個信箱，這會讓駭客容易一手掌握你所有資訊，把不同用途的信箱分開，不但便於管理，也能降低資安風險。

3、更新軟體。手機和電腦系統廠商都定期會提供軟體更新檔，許多是修補已被駭客發現的漏洞，更新能降低被攻擊的風險。

4、使用手機要小心。如果是安卓系統的手機，安裝 App，會被要求跟功能毫不相關的權限，如手電筒程式要求存取通訊錄的權限，就要小心是不是間諜軟體，不要給 App 和用途無關的權限。也有駭客會製作假 App，安裝程式前一定要看清楚。

資料引用自財訊：防止駭客入侵 專家教你自保 4 招

弱密碼概念宣導。

弱密碼以字面意思解釋就是容易被暴力破解或是容易被猜出的密碼，密碼暴力破解指的是用機器快速重複地嘗試不同的密碼登入，而容易被猜出的密碼簡單可以被歸為幾類：

1. 用自己的個人資訊，包括生日、電話、身分證號碼，住址。
2. 用簡單的密碼，如鍵盤排列 1qaz@WSX，英文單字 welcome，一串數字 123456 等。
3. 用外觀相似的替換符號，如簡單英文變化:l->1，O->0，a->@，例如 p@ssw0rd 就屬這一類。
4. 密碼和登入帳戶有大部分相同，所以一個帳密被破解等於多個系統受害。
5. 工作用密碼和工作相關，如"台北捷運"對英文"w961o3ru,6mp4"，就是注音對應英文弱密碼。

如果工作內容或性質跟機敏資料有關，應該盡量避免使弱密碼，使用超長密碼(15 個字元以上)或加上雙認證機制，以避免帳號密碼輕易被重複嘗試成功，遭到駭客入侵。

補充資料：

美國密碼管理應用公司 Splashdata 發布「2018 年度最弱密碼」榜單(SplashData's Worst Passwords of 2018)：

- 1.123456 (順序或重複的字符)
- 2.password (常用的單詞)
- 3.123456789
- 4.12345678
- 5.12345
- 6.111111
- 7.1234567
- 8.sunshine(常用的單詞)
- 9.qwerty (鍵盤有順序字符)
- 10.iloveyou