定期更換密碼不見得比較安全

據 Ars Technica 報導，卡內基美隆大學電腦科學與公共政策教授、現任美國聯邦貿易委員會（FTC）技術長 Lorrie Cranor，日前在 BSides 資安研討會上指出，定期更換密碼對安全性並無太大幫助，甚至有許多研究顯示，常換密碼反而更不安全。

Cranor 引述北卡羅來納大學教堂山分校的一項研究，其中針對 7,700 多組定期更換密碼的帳號進行分析。結果發現，使用者定期更換密碼通常都有一套固定的「轉換」（transformation）模式。多數人仍是使用舊密碼，再加上小小的改變，例如大小寫變換、頭尾加個字母或數字，就變成新的密碼。

該研究利用資料中發現的轉換規則，開發一套演算法，能夠精準預測密碼變更。接著再使用這套演算法模擬真實線上攻擊，有 17% 的帳號在五次嘗試內即被破解。以高速電腦執行離線攻擊時，則有 41% 的新設密碼，在三秒內就破解。

另一項由加拿大卡爾頓大學進行的研究也指出，要求用戶經常更換密碼，對阻擋劊客攻擊的效果不大，反而徒增使用者困擾，弊大於利。

那密碼該如何設定才安全又好記？

美國資安及密碼學專家 Bruce Schneier 發文附和 Cranor，表示定期更換密碼並不是有效的辦法，並針對密碼安全提出一些建議，分別是：用「句子」轉成密碼好記又安全、善用密碼工具、不重複使用同組密碼、小心設定「安全問題」、使用二階段認證。

密碼攻擊不單是依字母和數字順序窮舉，而會從常用的密碼詞及各種可預測的規則進行猜測。一般人選密碼通常有跡可循，是用特定詞做詞根（常用單字、姓名、特定語音組合），前後加上數字（例如 1 或 123456）、日期、固定字串（如「abc」）或符號（如「!」）。另外，破解密碼時也會嘗試常見的代換，例如用 $ 取代 s、用 @ 取代 a、用 1 取代 l。透過這些規則建立密碼詞典和演算法進行攻擊，往往能迅速破解大部分的密碼。

Schneier 建議好記又比較安全的方法是用句子轉為密碼，例如：This little piggy went to market 可以轉成「tlpWENT2m」；或是 When I was seven, my

sister threw my stuffed rabbit in the toilet 轉成「WIw7,mstmsritt...」。這類組合易記憶、個人化，也不會出現在密碼詞典中，因此不易猜測。

另外一招是用密碼管理工具（例如 Password Safe），可設定全亂數、不可記憶、非單純英數組合的密碼。

Schneier 最後提供四項建議：

1. 千萬別重複使用同一組密碼：即使選了安全的密碼，有的網站仍可能因本身防護能力不足而洩漏。若有人拿到這組密碼，可能進而破解你在其他網站或應用服務的帳號。
2. 不必浪費力氣定期更新密碼：定期換密碼弊大於利。除非認為帳號密碼可能被破解，否則沒必要更換。
3. 小心設定「安全問題」：大家總不希望忘記密碼時的備案救援系統，比密碼本身還好破解。使用密碼管理工具還是明智的選擇。再不然就是把密碼寫在紙上，收在安全的地方。
4. 若網站提供二階段認證，請認真考慮使用：幾乎保證能提高安全性。