

## 善用「輕推理論」養成網路衛生習慣

109 年 12 月 24 日

教育部全民資安素養網

資訊安全的術語當中，許多都是借鑒於醫學，而不論是資訊安全或醫學都有一個共通點：想要得到良好的成果，就需要盡可能讓多數人練習正確的行為，直到他們內化成習慣。例如，在每個人小時候，家長都會教導我們洗手與刷牙等基本的衛生常識，並且透過一系列的提示與技巧來鼓勵我們。根據「輕推理論」(Nudge Theory)，積極的強化與不著痕跡的建議將會影響人的行為與決策，以下列出幾項容易促使人們遵守資訊安全計畫的策略：

### 社會證明 (Social proof)

一般來說，當人們不知道如何行事時，通常會模仿他人的行為。因此，如果你將「最糟糕的密碼排行榜」提供給組織內的人員參考，多數人可能會認為：既然其他人都使用了這些糟糕的密碼，那麼擁有一組高強度的密碼似乎就不是那麼重要了。相反的，如果你告訴組織內的人員「同事之中有 70% 的人使用的密碼強度高於排行榜上的密碼」，就能鼓勵員工採取更安全的網路行為。

### 樂觀偏見 (Optimism bias)

有些高階管理者會認為，如果以前從未發生過某些事情，那麼它們就不太可能發生；也有些高階管理者會認為，閃電永遠不會擊中兩次，既然我們曾遭受過一次攻擊，應該就不會再發生第二次了。遇到這種情況時，可以透過向高階管理者提示其熟悉並深切關注的風險領域來克服這種偏見，並說明在沒有足夠防禦措施的情況下，可能如何加重風險，例如：可能造成嚴重的客戶個資外洩，甚至導致高階管理者的職位不保。

### 鼓勵與恐懼 (Encouragement vs. fear)

建立良好的網路使用習慣，通常意味著必須打破過往的不良習慣，這也是多數人所恐懼的，然而，當人們被鼓勵相信自己維護資訊安全的

能力時，他們往往會更加努力，從而在現實生活中，以及心靈層面上，都讓自己變得更加安全。

參考資料來源：

<https://www.scmagazine.com/perspectives/nudging-your-employees-towards-better-cyber-hygiene/>