

【政風宣導-公務機密宣導】網路攝影機資安防護建議

廉政檢舉專線：0800-286-586

1. 立即修改網路攝影機的預設帳號及密碼，並將密碼的強度提高，且避免與其它設備共用相同的密碼。
2. 不要在沒有任何資安防護措施(如防火牆等)保護的情況下，將網路攝影機直接曝露在網際網路上。
3. 不要將網路攝影機放置在主要網路上，以免駭客藉由入侵網路攝影機而進入主要網路，造成其它系統受害。
4. 網路攝影機的作業系統及韌體也可能存在資安漏洞，因此關注廠商所公布的漏洞修補程式並及時更新，可杜絕相關的資安漏洞。
5. 使用 SSL 或等效的安全通訊協定對網路連線進行加密，以防範中間人攻擊並避免機敏資料在傳送過程中遭竊。
6. 使用支援影像加密的網路攝影機，以避免有心人士藉由對網路攝影機的臨時物理接觸，而獲取儲存在記憶卡中的影像內容。
7. 使用支援雙因子認證 (Two-factor authentication, 2FA) 的網路攝影機，可以大幅降低網路攝影機遭駭客入侵的機率。
8. 注意網路攝影機安置地點，避免鏡頭對著需要高度隱私的區域，對於可經由遠端控制鏡頭旋轉角度的網路攝影機更是要特別留意。
9. 廉價的網路攝影機通常不會考量太多的資安要求與細節，因此價格不應是採購的主要考量。

【資料來源：摘錄自 TWCERT/CC 網站】