

專家的話：打造智慧家庭慎防網安風險



隨着5G技術的普及，人們生活追求智慧家庭(Smart Home)，現時很多家電廠商都朝智能家電方向研發生產，並推出APP方便消費者遠程操控，但在使用時又有哪些事項要注意？今期《澳門消費》請來澳門電腦商會歐家輝理事長與大家分享使用智能家電須注意的問題。通過本次訪談，希望消費者能更加重視智能家電APP及Wi-Fi網絡的安全問題，提高自我保護意識，確保個人信息及家居安全不受侵害。

1. 請問消費者在使用或安裝APP時，有哪些地方要注意？

首先應確保從官方或可信來源下載APP，避免安裝來路不明的應用程式，以防惡意軟件入侵。在安裝前，應仔細閱讀APP的權限請求，確保其請求的權限與其功能相匹配，避免過度授權。最後須定期更新APP及相關系統，以修補可能存在的安全漏洞。

2. 在家居的Wi-Fi設置上，有哪些地方要注意？

在Wi-Fi密碼的設置上，應使用數字、大小寫英文字母及符號的組合，避免使用過於簡單的密碼，如“123456”或“password”等，另外可考慮啟用WPA2或更高級的加密方式，提升網絡安全性。最後須定期檢查並更換Wi-Fi路由器密碼，以防被破解，關閉不必要的遠程管理功能，減少被攻擊的風險。

3. 現時不少消費者都會使用家用攝像鏡頭，又或使用具攝像鏡頭的智能家電，在使用相關產品時有什麼地方需要注意？

使用攝像鏡頭時須注意鏡頭的位置和方向，確認影像是否能拍到預定的目標，另外要避免拍攝到過於私密的區域。不要隨意將攝像鏡頭的登錄信息分享給他人，以防被窺伺或惡意控制。同時須定期檢查攝像鏡頭的安全設置，確保其未被非法入侵。

4. 在使用APP時，在個人資料保護方面又有哪些地方要注意？

密碼的設置是第一道防線，其次，不要在APP中存儲過於敏感的個人信息，如銀行卡號、身份證號等，並定期查看APP的隱私政策，確保其未將個人信息泄露給第三方，另外可考慮使用生物認證功能，最後如發現APP存在安全風險，應立即停止使用並聯繫廠商處理。

5. 當懷疑網絡被入侵，可以怎樣處理？

可先留意有關設備或應用程式廠家有沒有安全檢測或建議，另外當懷疑網絡被入侵時，可先關閉或重新安裝有關設備或應用程式，並立即更改登錄密碼。最後可聯繫網絡服務供應商或相關技術專家，尋求專業的技術支援。 