

115 年 7 月公務機密維護宣導

IoT 裝置安全指南

IoT (Internet of Things 物聯網) 裝置在我們身邊隨處可見，除了家用電器如掃地機器人、智慧家電，也包含許多在辦公場域常見的裝置，像是監視器、多功能事務機、門禁系統、空調與電力監控設備、智慧燈控等等，這些裝置能提高工作效率，但也可能帶來資安風險。

☆☆☆ IoT裝置常見風險 ☆☆☆

1. 未更換出廠時的預設帳號密碼。
2. 長期未進行韌體或安全更新。
3. 所有設備皆設置於同一網段或 Wi-Fi 環境。
4. 為了管理便利使用公開 IP 提供遠端存取。

◇◇◇ 如何保護IoT裝置 ◇◇◇

1. 正式使用連網前，一定要把預設帳密換掉，並設定夠強的密碼。
2. 主動檢查裝置廠商是否釋出更新版本，並安排定期檢查日更新韌體與系統。
3. 盡量把 IoT 裝置與內部核心系設置在不同的網段，避免一旦遭駭入，擴散至內部重要業務。
4. 透過防火牆限制 IP 與裝置聯絡，開啟日誌記錄追蹤存取軌跡。
5. 注意廠牌及產地，選購值得信賴的品牌。

資料來源：摘錄自 國家資通安全研究院出版「資安星際指南：網路安全輕鬆學」