赴中使用手機

資安署呼籲
強化防護措施

這些風險你都知道嗎?

moda 數位發展部 Ministry of Digital Affairs

七大資安風險示警

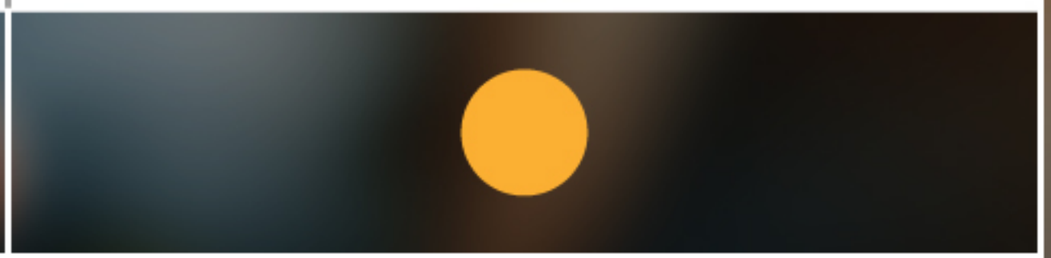
國人赴中使用手機資安風險

情境	一般民眾風險 隱私權	政府公務員風險 國家安全
台灣電信原號漫遊	🔵	🟡
使用當地公共 WiFi	🟡	🔴
當地 SIM / eSIM	🟡	🔴
USB 公用充電座	🟡	🔴
手機被迫離身情況 EX:海關安檢	🟡	🔴
安裝當地軟體 EX:微信/支付寶/滴滴等	🟡	🔴
當地購機 / 中製手機	🟡	🔴

moda 數位發展部 Ministry of Digital Affairs

🔵 還算安全　🟡 風險較高　🔴 風險極高

台灣電信原號漫遊

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

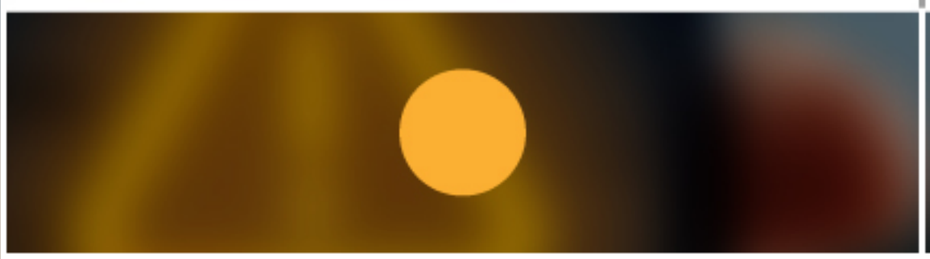
⚠風險 使用國內電信業者提供的原號漫遊服務，通訊內容將以加密方式傳輸，較使用當地SIM卡或eSIM安全；但漫遊中方仍可取得手機識別碼(IMEI)及GPS位置等資訊。

ⓘ建議 民眾開通漫遊比使用當地門號安全；如為公務員，建議開啟飛航模式，於必要時才進行連網。

moda 數位發展部 Ministry of Digital Affairs

還算安全　風險較高　風險極高

使用當地公共 WiFi

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

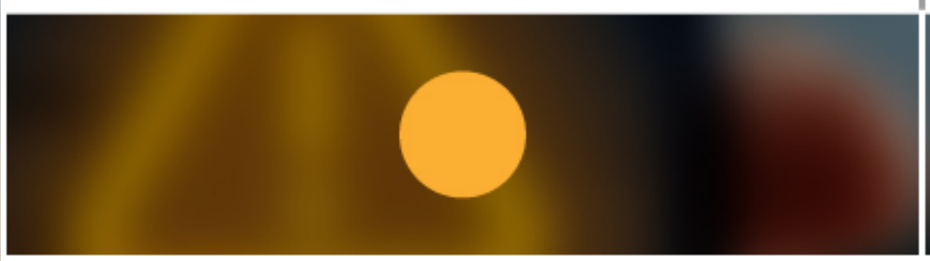
⚠風險 公共WiFi難以確認安全性，也經常成為駭客攻擊目標。

ⓘ建議 民眾儘可能避免使用當地公共WiFi；如為公務員，則禁用公共WiFi，避免公務資料遭竊取。

moda 數位發展部 Ministry of Digital Affairs

還算安全　風險較高　風險極高

當地 SIM / eSIM

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

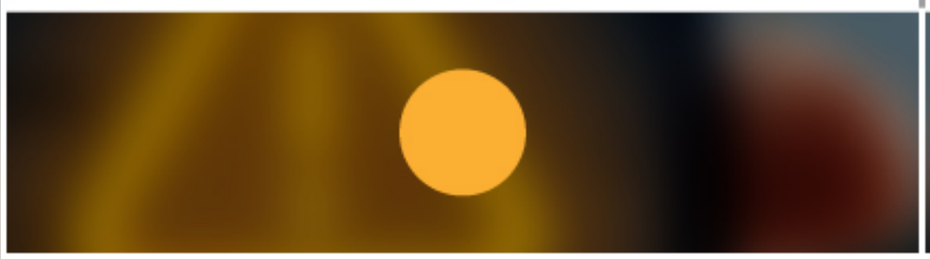
⚠風險 中國當地SIM卡或eSIM為「實名制」，一旦辦理使用，等同於將自身之身分、位置及網路活動暴露予中國政府之網路審查及監控機制。

ⓘ建議 民眾儘量以國內業者原號漫遊作為上網方式；公務員更應避免，僅於必要時以漫遊方式連網。

moda 數位發展部 Ministry of Digital Affairs

還算安全　風險較高　風險極高

USB 公用充電座

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

(Juice Jacking)

⚠風險 惡意設置的充電座可在使用者充電時將惡意軟體植入。

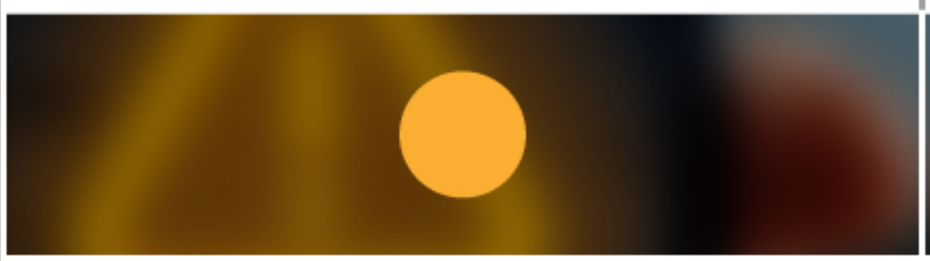
ⓘ建議 無論民眾或公務員，應使用自備的行動電源與充電器，避免遭駭或遭竊取資料。

moda 數位發展部 Ministry of Digital Affairs

還算安全　風險較高　風險極高

EX:海關安檢

手機被迫離身情況

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

⚠風險 透過專用設備，能在幾分鐘內提取通訊錄、簡訊、通話紀錄、甚至已刪除的檔案。

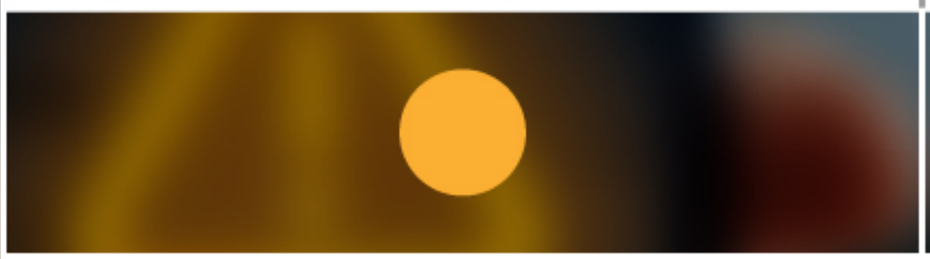
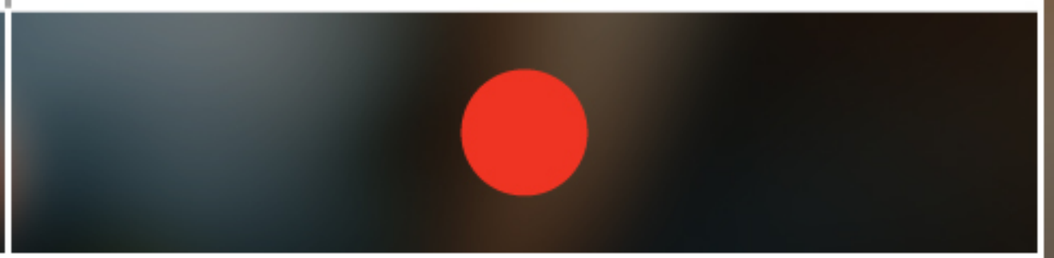
ⓘ建議 手機若因故離身，或遭搜查或留置，建議返國後立即重置系統，以降低遭安裝監控軟體之風險。公務員赴中前，應確保手機內無留存公務相關資訊，且避免在中國聯絡公務，以避免公務資料外洩或遭不當監聽。

moda 數位發展部 Ministry of Digital Affairs

還算安全 風險較高 風險極高

安裝當地軟體

EX:
微信/支付寶/滴滴等

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

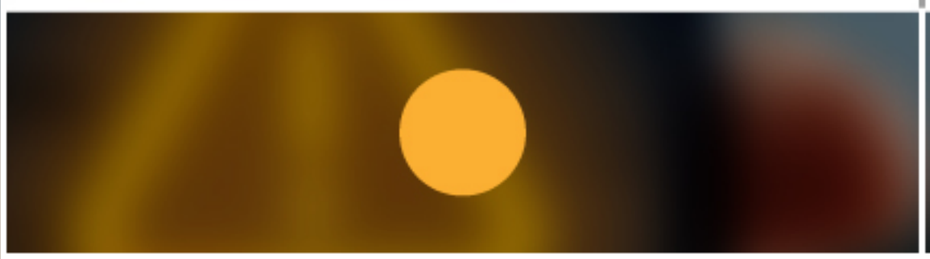
⚠風險 中製APP可能要求存取通訊錄、麥克風、相機、位置等與APP功能無直接相關之系統權限，安裝後會增加個人隱私與資料外洩風險。

ⓘ建議 勿安裝中製APP，公務完全禁止。

moda
數位發展部
Ministry of Digital Affairs

還算安全　風險較高　風險極高

當地購機 / 中製手機

一般民眾風險(隱私權)	政府公務員風險(國家安全)
	

核心風險分析與應對建議

⚠風險 中國販售或中牌手機有可能被安裝後門或監控軟體，其資料亦可能傳往中國當地資料中心，因此中國販售或中牌手機有極高資安風險。

ⓘ建議 勿購買當地手機或中牌手機，公務使用完全禁止。

moda 數位發展部 Ministry of Digital Affairs

還算安全　風險較高　風險極高