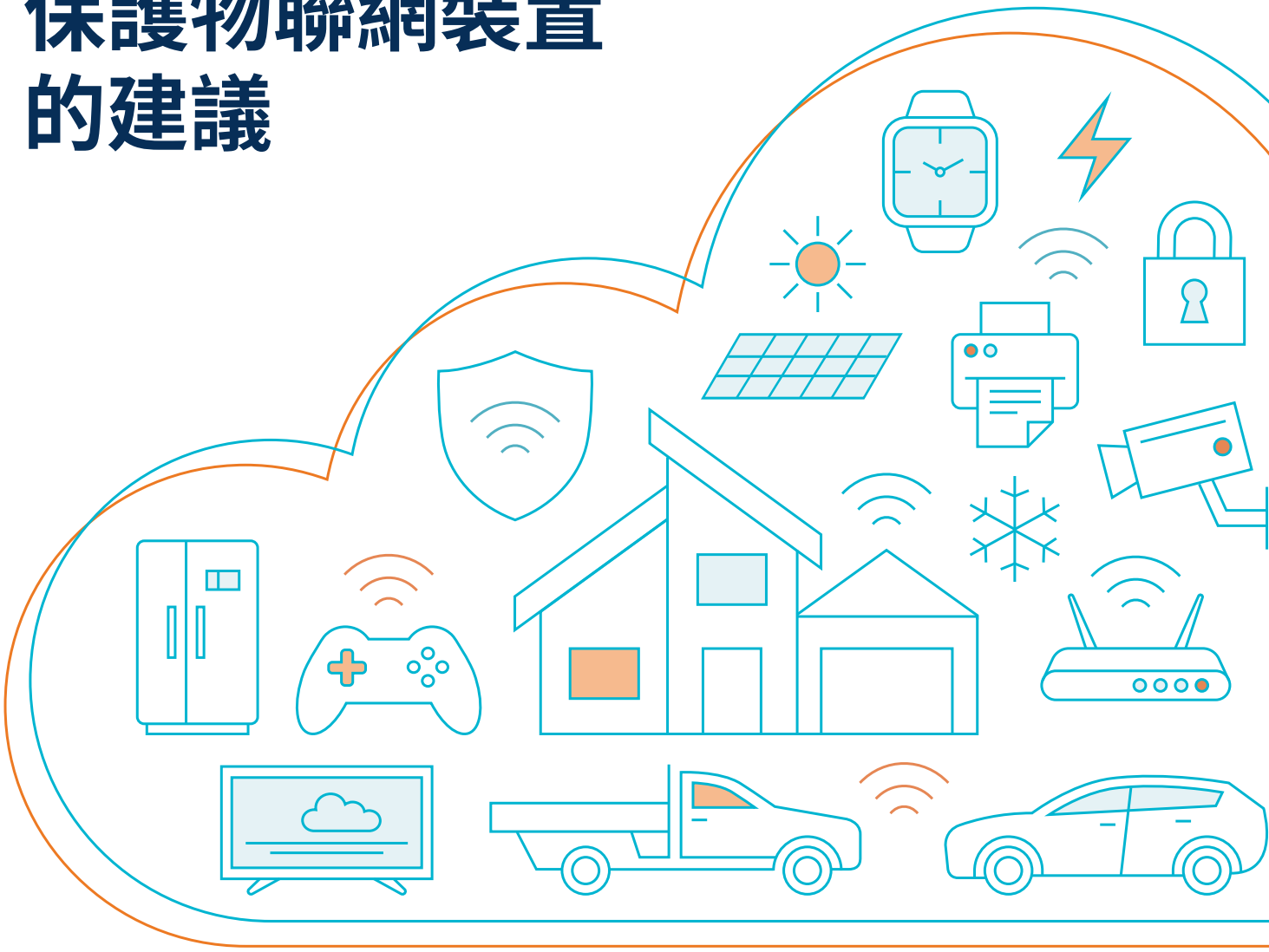
保護物聯網裝置的建議



澳洲網絡安全中心撰寫了本建議，以幫助社區人士安全地購買和使用物聯網 (IoT) 裝置。物聯網裝置是指具有網絡連線功能的日常用品，例如嬰兒監視器、無人機、保安攝影機、智能電視和太陽能逆變器。家用和商用的物聯網裝置，通常使用 Wi-Fi 或流動電話網絡 (例如 4G 或 5G)，以連接到互聯網。

澳洲家庭和企業中常見的許多物聯網裝置在設計時，並沒有考慮到安全性，導致裝置成為網絡攻擊和入侵的弱點，讓網絡犯罪分子在未授權的情況下存取您的裝置和個人資料，用作惡意目的。

購買物聯網裝置前

購物前的選購過程非常重要，因為各製造商的裝置在安全性方面或有不同。購買前，請先比較不同製造商出售的類似裝置。應考慮的事項包括：

1. **該裝置是否由知名且信譽良好的公司製造，並在知名且信譽良好的商店出售？** 知名且信譽良好的公司在製造產品時，會較重視產品安全性。知名且信譽良好的商店，較可能只會出售來自知名且信譽良好公司的裝置。他們對供應鏈有更嚴格的監管，確保裝置會按製造商的要求送達至客戶。

2. **能否變更密碼？** 更改密碼是一項明智之舉。然而，若裝置的預設密碼安全性較弱，此舉就顯得尤其重要。安全的裝置設有獨特、難以預測、複雜且無從猜測的密碼，因為攻擊裝置的最簡單方法，就是針對安全性弱的預設密碼。

3. **製造商會否提供更新？** 製造商在發現裝置有漏洞時，提供更新以修補漏洞的是非常重要的。例如，如果裝置上的軟件包含已知漏洞，或駭客開發出新的方法以攻擊該裝置，就需要進行更新以作修復。

4. **裝置會收集什麼數據，及會與誰分享？** 有關將收集什麼數據，以及如何使用這些數據的資訊，應詳列在製造商的網站或其隱私權政策中。應時刻留意網上或流動應用程式所收集的資訊。

5. **裝置是否僅執行您所預期的操作？** 購買功能超出所需的裝置（包括網絡連接），或能會降低您的安全性。您不會使用的裝置功能，不但無法提供益處，反而可能增加裝置遭受到攻擊的風險。

物聯網裝置

設定裝置時，請記住幾個簡單的問題，能幫助您確保網絡和資料的安全。

1. **該裝置有連接到網絡的需要嗎？** 並不是所有可以連接網路的裝置都應該連接，因為未有連接到互聯網的裝置，其被攻擊的風險相對較低。如果您不打算使用需要連接到互聯網的功能，就應考慮裝置是否需要連線。

2. **該裝置是否位於安全的地方？** 若裝置無須安裝在高風險區域，將其安裝於安全位置可以減低實體被入侵的風險。

3. **我應否更改預設的使用者名稱和密碼？** 使用強密碼或密碼短語是非常重要的。如果裝置的預設密碼並非獨特、難以估計、複雜且無從猜測的密碼，則有需要更改此密碼。預設的使用者名稱和密碼或會被收集並發佈到網絡上，使您的裝置較易受到攻擊。

4. **我的 Wi-Fi 網絡設定是否安全？有否安全密碼？** 保護您的 Wi-Fi 網絡和路由器，使攻擊者更難存取您的裝置和網絡。

多做一步

在路由器上另設一個只供物聯網裝置使用的 Wi-Fi 網絡，您的 Wi-Fi 路由器可將此網絡設為「訪客」網絡。如果您的物聯網裝置不需互相通信，請啟用「客戶端隔離」功能。將您的物聯網裝置與敏感資料隔離，確保物聯網裝置即使被入侵，也沒有權限存取其他裝置或資料。

5. **是否已關閉不必要的裝置功能？** 若您的裝置具有不需要或不必要的功能（例如相機或麥克風），則應盡可能停用。

多做一步

尋找關於啟用從本地 LAN 或 WAN／互聯網遠端存取裝置 Web 管理介面的設定。除非您需要遠端存取，否則應設定為本地 LAN。

維護物聯網裝置

一旦您的物聯網裝置設定完成並開始使用後，請緊記下列重要事項。包括：

1. **定期重新啟動您的裝置。** 如果物聯網裝置開始變得緩慢或無法運作，可能是病毒所致。大部分惡意軟件存在於記憶體中，可以透過重新啟動裝置（即關機再開機）輕易移除。若重新啟動後仍運作緩慢或無法運作，請嘗試恢復原廠設定，但請注意，此舉會清除使用者資料和個人化設定。

2. **定期更新。** 某些裝置會自動套用更新。對於那些未有更新的裝置，請定期留意製造商的更新資訊，在有更新時立即套用。當裝置不再獲得更新時，應考慮升級到較新且有更新支援的裝置。若發現新的安全漏洞，而裝置未能取得安全更新，則該裝置將無法受到保護，或可能會對您的網絡、私隱和資料構成風險。

3. **當裝置未被使用時，請關閉電源。** 長時間讓未使用或未受監控的裝置保持開啟並連接至Wi-Fi網絡，可能會提高其遭受攻擊的風險。若要自動操控開關，可使用具時間設定功能的電源插座，於指定時間內為裝置供電。

4. **留意每月的網絡使用量或帳單數目有否出現大幅增加。** 網絡使用量或帳單費用若有大幅增加，可能表示您的裝置已被入侵。除非貴機構的 IT 部門需就此作調查，否則應恢復原廠設定（注意此舉會清除所有使用者資料和個人化設定），然後更改您的密碼。

處置物聯網裝置

處理裝置（丟棄或出售）或會讓他人輕易取得您的個人資訊或數據。預防此類情況的方法包括：

1. **刪除所有資料和個人資訊。** 製造商應會提供方法，讓您從裝置和相關應用程式中刪除數據和個人資訊。刪除您的個人資訊，可確保您在處理裝置後，無人能存取內容。如果不再需要使用該物聯網裝置，應刪除相關的網上帳戶。

2. **將裝置恢復原廠設定。** 恢復出廠設定是為了清除本機儲存中的資料並將密碼、使用者名稱和設定重設成預設值。請參閱裝置的使用者手冊或製造商的網站，了解如何恢復原廠設定。

3. **將裝置與流動電話及其他裝置解除連接。** 若要處置的裝置仍可存取您其他的裝置、內部網絡或線上帳戶，可能會讓他人取得存取權限。應檢查您的其他裝置，確保與被處置的裝置間的連結已被刪除。 移除不再需要的流動應用程式的權限。

4. **移除連接到裝置的所有可移除媒體（例如USB儲存裝置、記憶卡等）。** 可移除媒體可能包含執行恢復出廠設定後也未有刪除的個人數據，所以應將其實體移除、銷毀，並與裝置分開處理。

尋求協助

請透過電郵 asd.assist@defence.gov.au 聯絡澳洲信號局轄下的澳洲網絡安全中心，或致電 24/7 熱線 **1300 CYBER1 (1300 292 371) 尋求緊急援助。**

在 ReportCyber 舉報網絡罪案，網址為 www.cyber.gov.au/report

如果您的身分遭到盜竊，請聯絡 IDCARE，網址是 www.idcare.org

請瀏覽 www.cyber.gov.au 以獲取對您和您家人有用的建議。註冊免費的 ACSC 警報服務，了解最新的網上威脅。

讓澳洲成為網絡連接最安全的地方。

如需網絡安全建議，請瀏覽 www.cyber.gov.au

免責聲明

本指南的內容只屬一般性資料，不應被視為法律建議，或是在任何特定或緊急情況下依賴作為幫助。在任何重要事項上，您都應該根據個人情況，尋求適當的獨立專業建議。

若因依賴本指南的資訊而引致任何損害、損失或費用，聯邦政府是不會承擔任何責任或義務的。

如需了解詳情或通報網絡安全事件，請聯繫我們：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

此號碼僅適用於澳洲境內。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre