Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

小企業網絡安全指南

內容複雜程度
簡易 ●○○

cyber.gov.au

引言

對於小企業來說，即使是一件微小的網絡安全事件，也可能帶來毀滅性的影響。本指南內包含的基本安全措施，是有助保護你的企業免遭常見的網絡安全威脅。首先，我們建議採取以下三項措施：

- 開啟多重身份認證
- 更新你的軟件
- 將你的資料備份

本指南可能包含與你的業務無關的措施，又或是你的業務可能有更複雜的需求。在看畢本指南後，我們建議小企業實施 **八項必要措施** 中的成熟級別一。如果你對此建議或更廣泛的網絡安全有疑問，我們建議你向資訊科技專業人士或值得信賴的顧問諮詢。

請瀏覽 cyber.gov.au 以閱讀我們的完整指南，包括每項措施的操作建議。

目錄

對小企業的威脅

詐騙短訊

「詐騙」是網絡罪犯針對小企業的常見方式。他們的目標是欺騙你或你的員工去：

- 匯款或發送禮品卡
- 點擊惡意鏈接或附件
- 洩露如密碼等敏感資料

網絡罪犯可能會試圖通過電子郵件、短訊、電話和社交媒體，向你的企業進行詐騙。他們通常會假裝是一名你信任的人或一個組織。

網絡釣魚攻擊

小企業特別擔心的是 **網絡釣魚攻擊** 。這些詐騙行動通常會有一個虛假網站的鏈接，而該網站會鼓勵你登錄賬戶或輸入詳細的機密資料。

網絡釣魚攻擊通常會竊取你的賬戶密碼。網絡罪犯經常使用這種方法來「接管」小企業的社交媒體賬戶及勒索贖金。

減輕風險方法

如果訊息是來自一個認識的實體，但看起來有可疑，便請謹慎行事。單獨聯繫此人或企業，以查證訊息真偽。使用通過合法源頭（例如瀏覽該企業的官方網站）找到的聯繫方式，而不使用可疑訊息中的聯繫方式。

使用以下資源來了解有關識別詐騙和網絡釣魚攻擊的詳細資訊：

- 識別及舉報詐騙事件
- 了解如何識別網絡釣魚詐騙行為
- 檢測社交工程訊息

案例分析：

一家快遞公司的員工收到一封來自公司一名行政人員的電子郵件，要求購買 6 張 500 元的萬事達預付信用卡。這名行政人員告訴她要保密，因為這些卡將發給員工作為禮券。而在購買後，員工要拍攝這些信用卡的前後兩面，並發送給這名行政人員，來作為已購買的證明。

該員工按照指示前往郵局，並使用她的個人信用卡購買禮品卡。她回覆行政人員的電郵，並發送了禮品卡的照片作為證明。

從郵局回來後，她將實體信用卡交給行政人員，但這名行政人員卻對此毫不知情。經審查後，**所有有關禮品卡的電郵都來自一個隨機電郵地址，而不是來自該名行政人員的合法電郵賬戶。這是一個騙局。**

電子郵件攻擊

除了網絡釣魚等詐騙之外，針對小企業的常見電郵攻擊亦包括**企業電郵入侵**(BEC)。犯罪份子可以通過使用被入侵的電郵賬戶或其他方式（例如使用與真實企業相似的域名）來冒充企業代表。除了竊取資料之外，這些攻擊的目標通常是欺騙受害者轉錢到詐騙者的銀行賬戶。

減輕風險方法

對抗電郵攻擊的最佳防禦措施就是培訓員工及提高他們的警覺。確保你的員工知道要經常謹慎對待包含以下內容的電郵：

- 付款請求，特別是關於緊急或逾期情況。
- 更改銀行的詳細資料。
- 電郵地址看起來不太對勁，例如是域名與供應商的公司名字不完全匹配。

儘管這些攻擊可能會帶來極大的破壞，但減輕風險的措施卻很簡單，而且幾乎不需要任何成本。**當職員收到這類電郵時，減輕風險的最有效措施便是致電發件人，來確認電郵的真偽。**請勿使用在電郵發送給你的聯繫方式，因為它們可能是具有欺詐性。為員工引入一個正式流程，讓他們在收到付款請求或銀行資料更改時，可以依循來處理。

了解如何使用以下資源，來保護你的企業免遭企業電郵入侵（BEC）的詐騙和電郵入侵：

- 企業電郵入侵
- 保護你的企業免遭電郵詐騙和電郵入侵
- 如果你的企業成為電郵詐騙或電郵入侵的目標，該怎麼辦？

案例分析：

一家小型建築企業收到供應商發來的電郵，稱他們已更換銀行，供應商提供了發票付款的新賬戶資料。由於這電郵看似合理，**故此建築企業沒有致電供應商來確認更改銀行賬戶資料的事情。**

該企業支付了供應商一張超過$70,000的發票。第二天，另一名員工誤將同一張發票再次支付，另外支付了$70,000多的款項，總計有超過$ 150,000 支付到新的銀行賬戶內。

當該企業致電供應商詢問是否可以退還重複支付的款項時，供應商指出這些銀行資料是不正確的。在立即展開調查後，供應商發現公司的一個電郵賬戶已被黑客入侵，並正發送出具欺詐性的銀行賬戶資料。**最終沒有追回任何款項。**

惡意軟件

惡意軟件是指用以造成危害的惡意軟件的總稱，例如勒索軟件、病毒、間諜軟件和特洛伊木馬病毒等。惡意軟件可以：

- 竊取或鎖定你設備上的檔案
- 竊取你的銀行或信用卡號碼
- 竊取你的用戶名字和密碼
- 控製或監視你的電腦

惡意軟件可能會阻止你的設備正常運作、刪除或損壞你的文件，或容許其他人取用你的個人或商業資料。如果你的設備感染了惡意軟件，你可能很容易會受到其他一些攻擊。該惡意軟件還可能傳播到你的網絡內的其他設備。

你的設備可能會通過多種方式感染到惡意軟件，包括：

- 瀏覽被惡意軟件感染的網站
- 從互聯網下載受感染的檔案或軟件
- 打開受感染的電子郵件附件

勒索軟件

勒索軟件是一種常見且危險的惡意軟件，它會鎖上或加密你的檔案，使你無法再存取它們，勒索者會要求支付贖金（通常以加密貨幣形式）來恢復檔案的存取。網絡罪犯還可能威脅會在網上發布或出售數據，除非他們收到贖金。

減輕風險方法

雖然防病毒或保安軟件可以助你免受惡意軟件侵害，但沒有任何軟件是百份百有效的。員工必須對電郵、網站和檔案下載保持警惕，並要定期更新設備來確保安全。

請參閱以下資源，了解有關保護你的企業免受勒索軟件侵害的詳細資訊：

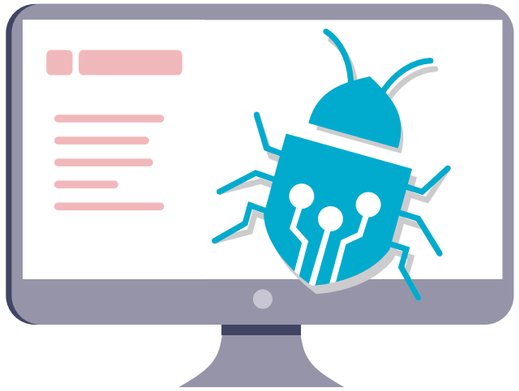
- 勒索軟件
- 保護自己免受勒索軟件攻擊
- 被勒索贖金該怎麼辦

案例分析：

一家汽車零件商店的員工一天早上上班，無法啟動他們的電腦伺服器。當他們的資訊科技提供商登入伺服器時，便發現一個打開的窗口，顯示所有電腦數據已被加密，有一條留言要求他們支付比特幣贖金來解鎖檔案。

插入電腦的一個備份硬碟亦已被加密，他們嘗試接上更多備份的硬碟，但檔案在數秒內都自動被加密。**在嘗試還原數據之前，他們未能清除勒索軟件，以致失去所有的備份檔案。**

最後唯一的選擇便是把伺服器出廠重置，以一個新系統重新運作。他們的企業丟失了多年的數據，不得不重新開始。



保護你的賬戶安全

開啟多重身份認證

多重身份認證(MFA)可以使網絡罪犯更難登入你的賬戶。

MFA 為你的賬戶增加另一層安全保障。這是保護你的賬戶不被他人登入的最有效方法之一，因此你應該盡可能使用它。登入你的賬戶的任何人士，都需要提供除你的用戶名字和密碼以外的其他資料，可能是來自短訊或身份驗證器應用程式的一個獨特代碼。如需了解詳情，請閱讀我們關於 MFA 的建議，網址為 **cyber.gov.au/mfa**。

✓ **從最重要的賬戶開始，盡可能啟用 MFA。**

實施存取管控

約束用戶存取權可以限制網絡安全事件所造成的損害。

存取管控是限制登入某些檔案和系統的一種方法，一般來說，員工不需要對企業內所有數據、賬戶和系統有完全存取的權限，他們只應獲准登入可以履行職責所需的範圍。

約束存取權將有助限制網絡安全事件所造成的損害，例如，採取了適當的存取管控後，假如員工的電腦中了勒索病毒，便可能只會影響少量檔案，而不會影響整個企業。

✓ **確保每個用戶只能獲得其崗位所需資源的存取權。**

使用強密碼或短語密碼

使用安全密碼或短語密碼來保護你的賬戶免受網絡罪犯侵害。

許多小企業因不良密碼行為而引致它們面臨網絡攻擊，例如，在多個賬戶上重複使用相同的密碼。你可以使用密碼管理器和短語密碼來創建強密碼。

密碼管理器就像一個虛擬的密碼保險箱，你可以使用它為你的每個賬戶創建和儲存強而**獨有**的密碼。如果你有很多賬戶，這將消除你牢記獨有密碼的負擔。你不必記住它們所屬的賬戶或密碼，因為這些都已記錄在你的密碼管理器內。

對於你定期登錄的賬戶或是不想儲存在密碼管理器中的賬戶，你可以考慮使用短語密碼來作為密碼。短語密碼是由隨機單詞組成的，例如是“crystal onion clay pretzel”。當你想要一個易於記住的安全密碼時，短語密碼是非常之有用。使用四個或更多的單詞隨機組合，並保持它的獨有性，**不要在多個賬戶重複使用同一個短語密碼**。如需了解詳情，請閱讀我們關於短語密碼和密碼管理器的建議，網址為 **cyber.gov.au/passphrases**。

✓ **使用密碼管理器來為你的每個重要賬戶創建和儲存獨有的密碼。**

管理共享賬戶

共享賬戶可能會削弱賬戶的安全及難以追踪惡意活動。

在小企業中，可能因為一些合理的原因而令員工需要共享賬戶，但就應該盡可能避免這樣做。當有多名員工使用同一賬戶時，可能會很難追踪是哪一名員工進行的活動，甚至更難以追踪入侵的網絡罪犯。除非你更改密碼，否則即使員工在離職後，也可繼續登入這些賬戶。

✓ **限制共享賬戶的使用及保護你在業務中使用的任何共享賬戶。**

保護你的設備和資料

更新你的軟件

保持軟件至最更新的狀態，是保護你的企業免受網絡攻擊的最佳方法之一。

「更新」是可以修復操作系統和其他軟件中的安全漏洞，從而使網絡罪犯更難入侵。由於時刻都會發現新的缺陷，故此不要忽視更新的提示。定期更新你的軟件，將減少網絡罪犯利用已知弱點來運作惡意軟件或入侵你的設備的機會。如果你需要幫助，ACSC已發布了有關更新的指南。

你的設備或軟件若太舊，則可能無法進行更新。如果製造商已停止為該產品提供更新支援，你應考慮升級到更新的產品，以確保安全。一些不再接受重大系統更新的例子，包括有**iPhone 7**和**Microsoft Windows 7**。

如需了解詳情，請參閱我們的更新指南，網址為**cyber.gov.au/updates**。

✓ **為你的設備和軟件啟動自動更新。**

使用保安軟件

防病毒和防勒索等保安軟件可有助保護你的設備安全。

使用保安軟件來檢測並刪除你的設備中的惡意軟件。你可以設置防病毒軟件，來定期掃描可疑檔案和程式。當發現有威脅時，你將收到警報，而那可疑的檔案將被隔離或刪除。

許多小企業可以**使用 Windows Security**來保護企業免受病毒和惡意軟件侵害，Windows Security是內置於使用Windows 10 和 Windows 11 的設備中，它包含免費的病毒和威脅防護。你還可以使用它來啓動你的設備上的勒索軟件防護功能。

如需替代產品和選項，請閱讀我們關於防病毒軟件的建議，可在cyber.gov.au上搜索*antivirus*。

✓ **設置保安軟件，以在你的設備上定期完成掃描程序。**

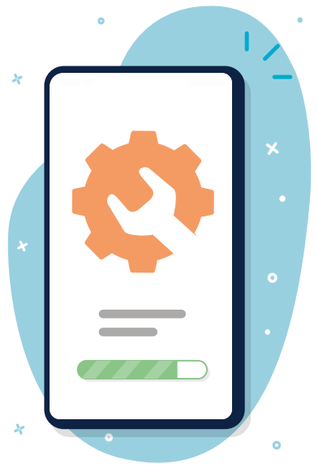
將你的資料備份

定期備份可以幫助你在資料遺失或洩露時恢復資料。

應該將重要資料備份，作為業務上的定期或自動做法。如果你沒有定期進行備份，在遭受網絡攻擊之後，便可能無法還原你的資料。

你可以使用多種方法和產品來將你的資料備份。有關業務備份的詳細建議，請閱讀我們提供的備份建議，網址為 **cyber.gov.au/backups**。哪一個是最佳選擇，會因個別商業而定，如果你不肯定，請向資訊專業人員查詢。

✓ **制定及實施計劃來定期備份你的資料。**



保護你的網絡和外部服務安全

在你的網絡中堵塞潛在的漏洞，以保護你的企業免受網絡攻擊。

你的網絡設備和服務可能成為網絡罪犯的主要目標。很多這類系統在保安方面可能會是很複雜，因此請與資訊科技專業人員討論以下的建議。

- **保護你的伺服器安全**如果你在家中或業務上使用NAS或其他伺服器，請特別注意保護它們的安全。這些設備是網絡罪犯的常見目標，因為它們通常用來儲存重要文件或執行重要功能。保護這些設備是需要很多減輕風險的策略。例如，確保定期更新所有伺服器或 NAS 設備是十分重要的。管理賬戶是應該使用強短語密碼或多重身份認證來保護其安全。
- **最大限度地減少面向外部的足跡**：審核及保護在你網絡內任何置於互聯網上的服務。這可能包括遠程桌面、文件共享、網絡郵件和遠程管理服務。
- **遷移到雲服務：**考慮使用有內置安全性的網上服務或雲服務，而不用自行管理。例如，使用網上服務來處理如電郵或網站託管等事務，而不用自己營運和保護這些服務的安全。
- **提高路由器(router)的安全性：**請遵循我們關於保護路由器的方法指南，包括更新默認密碼、為客戶或訪客打開「訪客」Wi-Fi、以及使用最強的加密協定。如欲了解詳情，請在 **cyber.gov.au** 搜索 *router*。
- **了解你的網絡供應鏈：**現代企業經常將多項服務外判。例如是使用託管服務提供商來維持資訊科技的工作。這些服務或提供商的安全問題可能會對你的業務產生重大的影響。有關網絡供應鏈風險管理的詳細建議，請查閱網絡供應鏈指南 (Cyber Supply Chain Guidance)，網址為**cyber.gov.au**。

✓ **與資訊科技專業人員討論保護你的網絡安全的方法。**

強化你的網站

網站是網絡攻擊的主要目標。

通過以下一些基本安全措施來保護你的網站免遭劫持：

- 使用多重身份認證或強密碼來保護你登錄網站的安全。
- 定期更新網站的內容管理系統和插件。
- 定期備份你的網站，以致在遭受網絡攻擊後也可以將它恢復。

ACSC 為網站所有者提供了額外的資源。在 **cyber.gov.au** 搜索這些資源：

- 你的網站快速成功策略
- 實施Certificates, TLS, HTTPS 和 Opportunistic TLS
- 域名所有者的域名系統安全
- 為「阻斷服務攻擊」(Denial-of-Service Attacks) 作出準備和應對

✓ **詳細閱覽ACSC關於網站安全的資源。**

在出售或處置掉你的設備前要將它們重置

陌生人有可能會取得你的舊設備內的數據。

如果你不安全地處置掉你的設備，網絡罪犯可能會取得裡面的資料，當中可能包括電郵、檔案和其他業務數據。在出售、交換或扔掉你的業務設備之前，請刪除它們裡面的所有資料.例如是通過恢復出廠設置，這樣便可刪除所有資料及將設備恢復到原始設置模式。

有關重置設備的建議，請閱讀我們關於如何安全處置你的設備指南，請在 **cyber.gov.au**搜索*dispose*。

✓ **在銷售或處置掉業務設備之前，須進行出廠重置。**

保持你的設備鎖定及確保它們在安全的地方

限制接觸你的企業設備，將減少這些設備遭遇惡意活動的機會。

限制實體接觸你的企業設備，是防止數據被盜或其他惡意活動的一個簡單方法。企業設備不應存放在未經授權的員工或公眾都可接觸到的地方。

使用安全管控措施來進一步保護你的業務設備。至少這些設備應使用短語密碼、密碼或生物識別技術鎖定。要確保這些設備有設置在短時間沒有活動便會自動鎖定的模式。

✓ **將設備配置為在短時間沒有活動後便自動鎖定。**

保護你的業務數據

你的企業持有的數據，對網絡罪犯來說是具有吸引力的目標。

數據洩露事件呈上升趨勢——不要讓你的企業成為受害者。了解你的企業保存哪些數據及保存在哪些位置，是甚為重要的。當你意識到這一點後，請使用本指南中的建議，來幫助保護你的數據免遭網絡罪犯入侵。一些小企業還可能根據法例而要承擔額外義務。

- **整合你的業務數據。**你可能將數據存儲在眾多設備或服務中。當數據不是集中在一起，你便有更多的系統需要加強保安並進行備份。系統眾多還可以為網絡罪犯製造更多的攻擊機會。如果可能，請將你的業務數據儲存在安全及會定期備份的一個中央系統。如果你的系統受到威脅，數據集中儲存便可能會造成更大量的數據外洩，因此請確保通過安全配置和限制存取，以充份保護這個中央系統。向一名資訊科技或網絡安全專業人士尋求建議。
- **了解你要保護數據的義務。**一些小企業在處理其收集的個人資料方面，可能需要承擔法律義務。請參閱澳洲資訊專員辦公室的小企業指南，以了解詳情，網址為：**oaic.gov.au**。如果你不確定，請諮詢法律專業人士。

✓ **了解你的企業持有的數據以及你要保護這些數據的責任。**

培訓你的員工

教育員工

員工具有良好的網絡安全習慣，便是你抵禦網絡攻擊的第一道防線。

你的員工應該具備網絡安全意識，包括以下主題：

- 常見的網絡安全威脅 - 如商業電郵外洩和勒索軟件
- 保護措施 - 包括強密碼或短語密碼、MFA 和軟件更新
- 如何察覺詐騙和網絡釣魚攻擊
- 企業特定政策（例如：報告可疑電郵或在付款前驗證發票真實性的程序）
- 緊急情況下該怎麼辦

ACSC 網站上有提供大部份主題的資源，網址為cyber.gov.au/learn。你可以考慮用其他方式來教育員工，例如正式課程或內部培訓。無論你如何決定，請記住網絡安全培訓不是一次性的要求，而應該是定期更新培訓。

✓ **確定如何在你的企業中教授網絡安全意識。**

制定應急計劃

應急計劃可以減少網絡攻擊對你的業務的影響。

在應對網絡安全事件時，分秒必爭。制定應急計劃，意味著你的員工可以花更少的時間來想清楚該做什麼，並有更多的時間採取行動。

在制定應急計劃時，請考慮以下問題：

- 你的員工報告潛在網絡安全事件的程序是什麼？
- 你要聯繫誰來尋求幫助？例如：資訊科技專業人員和你的銀行。
- 如何將事件傳達給你的員工、利益相關者或客戶？
- 如果任何關鍵系統離線，你將如何照常管理業務？

確保你的員工熟悉應急計劃，包括他們可能擔任的任何角色或職責。保留一份計劃印刷本，以防在系統離線時你需要看它。

✓ **制定網絡安全事件應急計劃。**

隨時了解情況

成為 ACSC 的夥伴，接收來自 ACSC 的最新資訊。

成為 ACSC 的夥伴，便可隨時了解最新的網絡威脅和漏洞。這項服務會向你發送每月通訊，並且在出現新的網絡威脅時，向你發出警報。

網絡安全是一個快速發展的領域。網絡罪犯在發現漏洞後幾分鐘內，就會積極利用漏洞犯案。隨時了解網絡安全形勢，將有助你的企業理解可能面臨的威脅，以及如何防範這些威脅。

✓ **向 ACSC 夥伴計劃註冊你的企業。**

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，依靠它作為幫助。在任何重要事項上，你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。

如需了解詳情或舉報網絡安全事件，請聯繫我們：

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

此號碼僅適用於澳洲境內。

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre