

# 詐騙和您的小型企業： 企業指南

Traditional Chinese



[ftc.gov/SmallBusiness](https://ftc.gov/SmallBusiness)





當詐騙者追擊您的企業或非營利組織時，您的聲譽和利潤都會受到傷害。那您的最佳保護呢？了解鎖定企業的詐騙跡象。然後，告知您的員工和同事要注意的事宜，以避免遭受詐騙。

---

- ▶ 詐騙者手法
  - ▶ 保護您的企業
  - ▶ 鎖定小型企業的常見詐騙
  - ▶ 其他有問題行為
- 

## ▶ 詐騙犯的伎倆

- 詐騙者會假裝是某個您信任的人。他們會冒充您知道的公司或政府機關來讓您付款。但這是詐騙。
- 詐騙者會製造緊迫感、恐嚇感及恐懼感。他們想讓您在找到機會確認其主張前採取行動。別讓任何人催促您付款或提供敏感性企業資訊。
- 詐騙者會要求您以特定方法付款。他們通常會要求電匯、加密貨幣或禮品卡形式的付款。切勿向任何利用此方法要求付款的人支付費用。這是詐騙。

## ► 保護您的企業

### 訓練您的工作人員

- 您的最佳防禦就是知情的工作人員。訓練員工不使用電子郵件傳送密碼或敏感性資訊，即使該電子郵件的寄件者看起來似乎是經理。向您的工作人員解釋詐騙的手法，並且鼓勵他們在懷疑有詐騙時與其同事討論。在 [ftc.gov/bulkorder](https://www.ftc.gov/bulkorder) 訂購本手冊的免費副本，然後分享給您的工作人員。

### 驗證發票和付款

- 確保設立清楚的採購和發票核准程序，並且要求您的工作人員仔細檢查所有發票。留意某人如何要求您付款，並且請您的工作人員一同注意。如果某人向您要求電匯、加密貨幣或禮品卡形式的款項，切勿付款。這是詐騙。

### 發現技術相關的詐騙

- 因為詐騙者通常會使用假的電話號碼，所以不要相信來電顯示。如果您意外收到簡訊或電子郵件，切勿點選任何連結、開啟附件或下載檔案。詐騙者會透過此方法將惡意軟體載入您的網路，或者試圖說服您匯款或分享敏感性資訊。詐騙者有時候甚至會駭進您認識的人的社交媒體帳戶，並傳送看起來很真（其實不然）的訊息。深入了解讓小型企業或非營利組織免受網路詐騙者和駭客侵害的資訊：請前往 [ftc.gov/cybersecurity](https://www.ftc.gov/cybersecurity) 查看小型企業的網路安全。

## 認識您要應對的對象

- 與新公司進行業務往來前，請搭配「詐騙」或「投訴」等詞上網搜尋該公司的名稱。閱讀其他人對該公司發表的想法。向您信任的人尋求建議。您也許能夠透過 **SCORE.org** 等計畫免費取得企業發展建議和諮詢。

## ▶ 鎖定小型企業的常見詐騙

### 偽造發票和未訂購的商品

詐騙者會製作假的發票，讓您以為自己為企業訂購產品或服務。他們希望向您支付帳單的人以為發票是真的，進而付款。其實這全都是假的。詐騙者也可能來電聲稱自己想「確認」現有訂單、「驗證」地址，或者提供「免費」目錄或樣品。如果您接受任何一點要求，未訂購的商品即會送貨到府，接著他們會施加高壓的付款要求。切勿付款。然後請記住，如果收到未訂購的商品，依法您有權保留該商品並免費使用。

### 線上刊登資訊和廣告詐騙

詐騙者會試圖欺騙您付款使用偽造企業名錄中不存在的廣告或刊登資訊。他們可能也會要求您為「免費刊登資訊」提供聯絡資訊，或者表示該通話只是為了「確認」您的資訊。稍後，您將收到高額帳單，接著詐騙者可能會利用先前通話的詳細資料（甚至是錄音）強迫付款。

## 企業和政府假冒詐騙

詐騙者會假冒某個您認識或信任的人，然後試圖嚇唬或催促您付款或向他們提供資訊。例如：

- 詐騙者以公用事業公司名義致電，因為（假的）帳單逾期，準備中斷您的瓦斯、供電或供水服務。
- 詐騙者表示他們是公務人員並威脅暫停您的營業執照、對您處以罰款，甚至是控告您。他們可能會聲稱這是因為您欠稅，或者需要更新執照或登記。
- 有些詐騙者會說服您購買工作場所的合規性海報，但其實可以向美國勞工部免費索取。
- 有些詐騙者會誘騙您付費申請所謂的企業補助，結果是假的政府計畫。
- 詐騙者會冒充美國專利及商標局，並且威脅如果不馬上繳清費用，您就會失去自己的商標。有些時候，他們會編造您有其他登記服務欠費未繳的謊言。
- 有些詐騙者會說他們是從科技公司致電，並威脅如果不馬上付款，貴企業的網站 URL 就會不見。

## 技術支援詐騙

技術支援詐騙一開始會是一通電話，或是螢幕上跳出警告訊息。詐騙者會假裝成知名科技公司的員工，並且告訴您電腦安全出現了問題。他們是為了拿到您的錢、存取您的電腦，或兩者都要。他們可能會要求您付費修復實際上不存在的問題、為您的企業註冊不存在或無用的

電腦維護計畫，或者偷偷潛入您的電腦網路，以便拿取他們可用於盜用身分的機密資料。

## 社交工程、網路釣魚及勒索軟體

網路詐騙者可能會誘騙員工匯款或交出機密或敏感性資訊，像是密碼或銀行資訊。一開始通常是網路釣魚電子郵件、社交電子郵件聯絡人，或是好像來自受信任來源的通話（例如，主管或其他資深員工），藉此製造緊迫感或恐懼感。有些電子郵件看起來可能像是日常密碼更新要求或其他自動化訊息，但其實會試圖竊取您的資訊。詐騙者可能也會使用惡意軟體鎖定組織的檔案，並且以此當作勒索贖金的手段。

## 企業輔導詐騙

有些詐騙者會銷售謊稱的企業輔導計畫，且通常會利用假的見證、影片、研討會簡報及電話行銷通話。他們會假裝承諾如果您付費使用其專有「認證」系統，即可取得驚人結果，進而讓企業取得成功。他們可能也會以低廉的初始成本誘導您，但這只是為了在日後要求數千美元做準備。實際上，詐騙者會讓初露頭角的企業家得不到他們尋求的協助，並且留下數千美元的債務。

## 改變網路上的評論

有些詐騙者會宣稱他們可以幫您的產品或服務換掉負面評論、新增正面評論，或者提升評分網站上的分數。但是，發佈假評論屬於非法行為。FTC 指導方針表示代言（包括評論）必須反映代言人的誠實意見和體驗。

## 信用卡處理和設備租賃詐騙

有些詐騙者會承諾更低的信用卡交易處理費率，或是更優惠的設備租賃費用。這些詐騙者會利用附屬細則、半真半假的陳述及完全的謊言，以便讓業主在合約上簽名。有些不良銷售代理人會要求業主簽署空白文件（請不要這麼做）。據悉有些人會在事後變更條款。要求銷售人員立即向您提供所有文件的副本。如果他們拒絕或承諾稍後再傳送給他們，這可能就是遇到詐騙者的跡象。

## 偽造支票詐騙

有些詐騙者會給您看似說得煞有其事的理由，使用支票多付錢給您。然後，他們會要求您將多餘的錢還給他們或其他人。但這是張假支票，即使您的帳戶中可能會顯示為「已清算」。當銀行發現該支票有問題，詐騙者早就拿到了您匯給他們的錢。您則擺脫不了償還銀行款項的處境。

## ▶ 其他有問題行為

詐騙者有時候會利用其他有問題行為掩飾，像是聲稱提供高薪的零工經濟工作，但之後卻無法履行他們的賺錢承諾。或者他們可能會試圖向您銷售不必要的服務，並且假裝聲稱您必須付費才能改善企業信用報告。而且在自然災害侵襲後，無牌承包商和詐騙者可能會做出虛假承諾，聲稱他們會利用快速維修、清理或清除殘骸讓您的企業恢復正常機能，但其實從未發生。

## ▶ 深入了解

- 如需保護貴組織免受詐騙侵害的詳細建議，請造訪 **ftc.gov/SmallBusiness**。
- 請前往 **ftc.gov/subscribe** 訂閱 FTC 企業部落格，隨時更新 FTC 的相關資訊。

## ▶ 舉報

- 如果您發現詐騙，請致電 **877-382-4357**，如果需要其他語言請按 **3**，然後按 **1** 選擇普通話，或造訪 **ReportFraud.ftc.gov**。
- 提醒您的州檢察長。如需聯絡資訊，請前往 **NAAG.org**。

## ▶ 參與

- 請記住：您的最佳防禦就是知情的工作人員。告訴您的員工詐騙的手法。
- 將本手冊分享給您的工作人員。
- 請造訪 **ftc.gov/languages** 下載本手冊的免費副本。

## 關於 FTC

FTC 致力於幫助小企業主避免詐騙、保護其電腦及網路並確保客戶資料的安全。若要查找小型企業的資訊，請造訪 **ftc.gov/SmallBusiness**. 您可以在此處查找有關小型企業的詐騙以及如何避免詐騙的資訊，以及小型企業的網路安全資訊，幫助業主確保其網路安全。

若要獲得小型企業的最新資訊，請訂閱 FTC 的商業部落格：**ftc.gov/subscribe**.



This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **[ftc.gov/bulkorder](https://www.ftc.gov/bulkorder)**.



**FEDERAL TRADE  
COMMISSION**

**[business.ftc.gov](https://business.ftc.gov)**

2023年7月