

# 2024 年全美小企業周開始;國稅局為全美企業家提供稅務資源和信息

IR-2024-123, 2024年4月26日  
華府 — 美國國稅局今天向企業家提供了有用的信息,以迎接即將到來的全美小企業周,慶祝和認可美國小企業對國家經濟做出的重要貢獻。

每年,美國小企業管理局(英文)都會率領舉辦全美小企業周,為企業家提供資源、福利和其它重要的創業信息。小企業主可以利用這些信息來創辦自己的企業。今年的慶祝活動主題為繼續打造全美小企業繁榮,將於4月28日至5月4日舉行。

美國國稅局是全美小企業周慶祝活動的合作夥伴,今年國稅局將展示大量資源,幫助小企業主學習和瞭解他們的稅務責任和福利。本周,國稅局將在其受歡迎的稅務提示(英文)電子新聞出版物以及國稅局社交媒體平台(包括 Facebook(英文)、X(英文)(以前稱為 Twitter)、LinkedIn(英文)和 Instagram(英文))上發佈有用信息。

下周,國稅局將分享幾個重要的稅務主題,以幫助小企業主的成長和發展:

4月29日,星期一。小型企業的最佳實踐 — 國稅局強烈鼓勵小型企業家利用 IRS.gov 上提供的眾多資源,瞭解如何創業並瞭解最佳實踐對於小型企業的成功至關重要。

4月30日,星期二。創辦企業時需要瞭解的信息 — 深入瞭解創辦新企業時需要考慮的關鍵因素。訪問創辦企業(英文)網頁,確保為創業之旅奠定堅實的基礎。

5月1日,星期三。謹防詐騙! — 美國國稅

局“骯髒十二條騙術”等!大多數網絡攻擊針對的是員工少於100人的小型企業。小企業主必須實施數據保護措施,並始終警惕與稅務相關的詐騙。

5月2日,星期四。為支持小型企業的稅務專業人士提供的建議 — 隨時瞭解國稅局的最新動態,並獲取為稅務專業人士量身定制的資源。

5月3日,星期五。期待意想不到的事情! — 國稅局可以在災難後幫助小企業! 國稅局關注的一個重點是減輕受聯邦宣佈的災難影響的納稅人的聯邦稅務負擔。國稅局與多個機構合作提供援助並協助救災工作。

尋求開辦小型企業涉及與稅務問題相關的幾個重要考慮因素:

### 如何獲得雇主身份識別號碼

大多數企業主都需要雇主身份識別號碼(EIN),這是一種永久的身份識別形式,在許多情況下必須用於提交稅表,並且可用於滿足各種業務需求,例如開設銀行賬戶。企業可以立即通過 IRS.gov 在線獲取 EIN,而且是免費的。

### 選擇企業架構

小企業主作為納稅人,在開辦新企業(英文)時必須決定最適合其企業的企業架構。他們選擇的企業架構決定了企業主每年提交的所得稅申報表的類型。一些常見的企業架構包括:

獨資企業(英文)。單獨擁有非法人企業的個人為獨資經營者。

合夥企業(英文)。合夥企業是兩個或兩個以

上的人之間開展貿易或業務的關係,每個人貢獻金錢、財產、勞動力或技能,並分享企業的利潤和損失。

公司(英文)。在公司中,潛在股東交換金錢、財產或兩者,以獲取公司的股本。

S型公司(英文)。S型公司是一家出於聯邦稅收目的而選擇將公司收入、損失、扣除和抵免轉嫁給其股東的公司。

有限責任公司(LLC)(英文)。有限責任公司可以被視為公司、合夥企業或所有者稅表的一部分(例如獨資企業),具體取決於有限責任公司及其成員的選擇。有限責任公司還可能受到州法規的約束,各州的法規有所不同。

### 瞭解企業稅

聯邦法律要求所有個人,包括小企業主,對所有收入納稅。這通常涉及小企業主和自僱業者按季度繳納預估稅款。如何繳納企業稅取決於創業者選擇的企業結構。以下是四種普遍認可的企業稅類型:

收入所得稅。除合夥企業外,所有企業都必須提交年度聯邦所得稅申報表;合夥企業必須提交稅務資料申報表。



# 全美小企業周:國稅局提醒小企業主小心數據安全,保護他們的企業、員工和客戶

IR-2024-128, 2024年5月1日

華府 — 在全美小企業周繼續開展之際,美國國稅局敦促小企業主落實數據安全保障措施,保護他們的財務、個人和員工信息免受詐騙和網絡犯罪分子的追捕。

國稅局不斷發現小企業和其他人面臨各種與金融和身份盜竊相關的騙局,這些騙局試圖獲取用於提交虛假小企業稅表、打劫商業銀行賬戶和創建被盜身份的信息。

例如,“網絡釣魚”和“魚叉式網絡釣魚”詐騙繼續針對小企業以及稅務專業人士和個人納稅人。小型企業仍然是 W-2 表格詐騙的目標,身份竊賊試圖誘騙公司領導者分享敏感數據。

“每年,美國國稅局發現有數千起試圖攻擊小企業主和其他納稅人的嘗試。這些騙局的受害者可能會面臨嚴重的財務後果。”國稅局局長 Danny Werfel 表示,“網絡犯罪分子是無情的,任何人都可能成為目標。企業主和個人保護自己的最佳方法是充分瞭解最新的騙局,持續保護他們的計算機和智能手機,並在家和公司安裝數據安全裝置以保護敏感信息。”

### 網絡犯罪分子全年無休

數據盜竊和網絡攻擊是全年威脅,它們可以在白天或晚上的任何時間利用詐騙和欺詐計劃來傷害個人和小型企業。網絡犯罪分子非常擅長掩蓋自己的踪跡,並且可以隱藏在世界任何地方。

他們利用人類行為模式和計算機系統竊取財務和個人信息並誘騙受害者。如果小型企業不能正確保護其計算機系統並對其員工進行智能數據保護實踐培訓,則所有者很容易成為想要闖入銀行賬戶和竊取身份的不良行為者的目標。

國稅局敦促小型企業界認真對待網絡犯罪的威脅,並瞭解保護其業務數據免受身份盜竊的重要性。他們應該採用強大的技術工具和服務來嚴格保護金融和貿易信息,並保護與客戶、員工和業務合作夥伴直接相關的數據。

網絡犯罪分子不斷尋找可利用的弱點。小企業主通過實施基本的網絡安全措施和培訓員工,可以顯著降低遭受代價高昂的攻擊的風險。這些攻擊可以針對企業最有價值的數據,包括:

信用卡和付款信息。數據泄露可能會損害企業的聲譽,並使所有者承擔欺詐費用。

企業和員工身份。被盜信息可用於多種犯罪,包括身份盜竊和欺詐。

稅務和財務信息。黑客可以利用這些信息提交欺詐性稅表,從而花費企業主的時間和金錢來解決問題。

為了保護商業投資、客戶和員工,小企業主儘早採取基本的網絡安全措施並保持警惕,掌握有關最新詐騙的信息。

詐騙者如何精準受害者:騙局、騙局和更多騙局

欺詐者和網絡犯罪分子是操縱人類行為的投機分子。他們利用潛在受害者與他人進行社交互動和自然的願望,竊取數據和身份。欺詐者使用電子郵件、短信和社交媒體等常見技術,通過一次性向數千個目標發送消息來直接竊取個人信息,或者讓受害者點擊嵌入的鏈接或附件,從而進行“網絡釣魚”。

使用電子郵件作為通過“網絡釣魚”操縱行

為的方法仍然是盜賊尋找潛在受害者的常用策略。小型企業應對與稅務相關的“網絡釣魚”電子郵件詐騙保持警惕,這些詐騙通常可以巧妙地編寫來欺騙員工打開有害的嵌入式鏈接或附件。我們鼓勵小型企業和消費者將與國稅局相關的詐騙郵件發送至 phishing@irs.gov。

W-2 表格盜竊騙局就是這樣的一個例子。雖然這些騙局的操作隨著時間的推移而演變和變化,但在最常見的操作中,竊賊冒充公司高級管理人員,向薪資員工發送電子郵件,要求提供員工名單及其 W-2,其中包含敏感的稅務和財務信息數據。隨著這些騙局變得越來越複雜,小企業可能不會意識到這已經成為稅務騙局的受害者,直到開始出現帶有員工姓名的欺詐性稅表。

對於遇到 W-2 騙局的雇主,有特殊的報告程序。請訪問身份盜竊中心的商業部分(英文)以獲取更多信息。

### 骯髒十二條騙術

國稅局每年都會發佈“骯髒十二條騙術”,列出了威脅小企業和其他納稅人的普遍存在的詐騙和欺詐計劃。這些威脅包括員工留任稅收抵免(ERC)可疑申請的不擇手段和激進推廣人。

這些可疑的員工留任稅收抵免申請常常使毫無戒心的企業和其它實體面臨處罰、利息,甚至可能因在不符合資格且無權獲得員工留任稅收抵免的情況下申請而面臨刑事起訴。

如果個人或小企業主懷疑自己可能成為受害者,可以參考“骯髒十二條騙術”中提供的信息。例如,企業仍然可以選擇撤回任何未處理的可疑員工留任稅收抵免申請,並應針對尚未支付的任何納稅期迅速進行申請撤回程序(英文)。

企業主可以將“骯髒十二條騙術”作為其自行研究的起點,進而從其它可信來源瞭解各種流行騙局。

目前,“骯髒十二條騙術”報告的影響小型企業的最嚴重詐騙之一是“新客戶”“魚叉式網絡釣魚”騙局。魚叉式網絡釣魚通過惡意電子郵件或短信針對特定個人、組織或企業。

在“新客戶”騙局中,網絡犯罪分子向已知稅務專業人士或企業主展示自己是新的潛在客戶,要求他們回復電子郵件。如果不知情的代報稅人或企業主做出回復,犯罪分子就會發送惡意附件或網站地址,這些附件或網站地址可能會危害受害者的計算機系統,並允許攻擊者訪問敏感的客戶和財務信息。以下是一些需要注意的危險信號:

語法上的奇怪之處。寫得不好、用詞不尋常的電子郵件是一個嚴重的危險信號。

可疑的請求。在驗證發送人的合法性之前,企業主應始終警惕任何異常請求或共享信息。

欺騙性電子郵件。詐騙者可以模仿以前的客戶電子郵件,使它們看起來很真實。不要被愚弄,請另外獨立驗證發送人的地址。

通過保持警惕並瞭解這些騙術,小企業主可以保護自己及其客戶免受“新客戶”騙局的傷害。謹慎總是比妥協好。

不要成為容易的目標,學習網絡安全基礎知識

強烈鼓勵小企業主儘可能多地瞭解網絡安全最佳實踐,即使日常信息技術保護是外包的。美國國稅局建議企業主實施美國聯邦貿易委員會發佈的最佳實踐(英文)。許多人都熟悉常識性

的習慣和技巧,但不要認為它們是理所當然的。適用於家庭的方法也適用於企業。

### 保護企業文件和設備:

更新軟件。這包括應用程序、網絡瀏覽器和計算機操作系統。設置為自動更新。

保護業務文件。離線、外部硬盤或雲中備份重要文件。還要確保安全地存儲紙質文件。

設置密碼。對所有筆記本電腦、平板電腦和智能手機使用密碼。不要將這些設備留在公共場所無人看管。

加密設備。加密包含敏感個人信息的設備和其他媒體。這包括筆記本電腦、平板電腦、智能手機、可移動驅動器、備份磁帶和雲存儲解決方案。

使用多重身份驗證。需要多重身份驗證才能訪問包含敏感信息的網絡區域。除了使用密碼登錄之外,這還需要其他步驟,例如智能手機上的臨時代碼或插入計算機的密鑰。

### 保護企業無線網絡:

保護企業路由器的安全。設置路由器後,更改默認名稱和密碼、關閉遠程管理並注銷管理員身份。

至少使用 WPA2 加密。確保路由器提供 WPA2 或 WPA3 加密並且加密設置已打開。加密可保護通過網絡發送的信息,使其無法被外部人員讀取。

### 讓智能安全成為常規措施:

需要強密碼。強密碼至少由 12 個字符組成,由數字、符號、大小寫字母組成。切勿重複使用密碼,也不要通過電話、短信或電子郵件分享密碼。限制登錄嘗試失敗的次數,以限制密碼猜測攻擊。

培訓員工。通過實施定期的員工培訓計劃來創建安全文化。隨時瞭解最新的數據安全風險和漏洞,並讓員工隨時瞭解情況。考慮阻止無視數據安全措施和培訓的員工訪問網絡。

設置一個計劃。制定保存數據、運營業務並在發生數據泄露時通知客戶的計劃。美國聯邦貿易委員會的數據泄露響應:企業指南(英文)提供了企業主在發生網絡泄露時可以採取的步驟。

有關企業主如何保護其投資、客戶和員工免受網絡犯罪分子侵害的更多信息,請訪問 FTC 的小型企業網絡安全(英文)。

如果小型企業成為身份盜竊的受害者,下一步該怎麼辦

國稅局還發佈了《表格 14039-B, 企業身份盜竊宣誓書》(英文)PDF,使小型企業可以在電子提

自雇稅。主要針對為自己工作的個人徵收的社會保障和醫療保險稅。納稅有助於個人的社會保障體系覆蓋。

就業稅。有雇員的小型企業必須繳納某些就業稅責任,並必須提交特定表格。

工商稅。工商稅針對各種商品、服務和活動徵收,根據具體稅種,可能會對製造商、零售商或消費者徵收工商稅。

### 選擇“納稅年度”

“納稅年度”是報告收入和花費的會計期間。小型企業可以選擇最適合其運營需求的納稅年度:日曆年。從 1 月 1 日開始到 12 月 31 日結束的連續十二個月。

財政年度。以除 12 月之外的任何月份的最後一天結束的連續十二個月。52 至 53 周納稅年度是指週期為 52 至 53 周但不必在每月最後一天結束的財政納稅年度。

### 保持良好的記賬習慣

保持良好的企業記錄(英文)不僅有助於準備稅表,還可以幫助小企業主準備財務報表、確定收入來源、跟踪可扣除費用和監控其業務進度。小企業主應保留其業務記錄至少三年。



**李侑真 Jane Y. Lee 國語,英語**  
 移民律師 Immigration Lawyer  
 614-452-4915 Call to Schedule an Appointment

**服務包括:家庭移民, 工作移民, 入籍申請, 豁免申請(Waiver), 庇護**

**PETERSON CONNERS LLP**  
 545 Metro Place South, Suite 435, Dublin, OH 43017  
 Web: www.petersonconners.com; www.attorneyjanelee.com



**老王裝修**

專業改造浴室、黏地板磚、鋪地板、室內裝修、沒有最好只有更好。

區域: 俄亥俄州各地區  
 電話: 347-420-1877

**注冊會計師事務所**  
 National Tax and Accounting Inc

公司地址: 92 Northwoods Blvd, STE A, Columbus, OH 43235  
 中英文電話: 614-962-0868 郵箱: fred@nationaltax.net 微信號: Nationaltax

成立於 1999 年, 具有豐富的稅務和會計經驗, 人力資源雄厚, 價格合理。多年來為公司、個人提供完善、精準的稅務申報和其它會計服務, 為客戶合理合法省稅。

事務所提供以下服務:

- \* 個人稅務申報
- \* 公司會計服務
- \* 員工工資及相關稅務
- \* 公司稅務申報
- \* 公司稅務計劃
- \* 公司成立登記註冊