



立即發佈：2022年3月22日

凱西·霍楚爾州長

霍楚爾州長提醒消費者留意俄羅斯入侵烏克蘭期間的詐騙和網路安全威脅

捐款給經過檢驗和信譽良好的組織，這些組織使用捐款為有需要的烏克蘭人提供救濟

州機構提供了許多保護您的敏感資訊，在日益嚴重的網路威脅下保持警惕的建議

凱西·霍楚爾州長今天就與弗拉基米爾·普京 (Vladimir Putin) 入侵烏克蘭有關的慈善詐騙和更嚴重的網路安全威脅向紐約民眾提供了建議。紐約州消費者保護部 (New York State Division of Consumer Protection) 獲悉了以支援戰爭受害者的名義要求捐獻慈善救濟金的欺詐性請求。鼓勵消費者在捐贈金錢或物資之前仔細評估任何金錢請求並驗證慈善機構。霍楚爾州長亦鼓勵紐約民眾在網路安全威脅日益嚴重的情況下，利用稅務和財政部 (Department of Taxation and Finance) 的安全建議，在網上發佈敏感資訊時保持警惕。在此之前，州長成立了[聯合安全行動中心 \(Joint Security Operations Center\)](#)，以作為地方、州和聯邦聯合網路工作的中心。

霍楚爾州長表示，「紐約是美國擁有烏克蘭人口最多的州，紐約民眾總是伸出援助之手來照顧有需要的人。」「但是，我們必須對那些試圖利用他人的善意實施欺詐的人保持警惕。在您慷慨地幫助我們的烏克蘭朋友和家人時，請記住，如果某些事情看起來可疑，那很可能就是可疑的。鼓勵您的朋友和家人，尤其是年長的親人，上網時保持警惕。」

每當災難發生時，騙子都會利用尋求幫助的人的心弦進行詐騙。入侵烏克蘭為騙子提供了建立虛假慈善機構或偽裝成引人注目的戰爭受害者的機會。其他騙子設計網站來模仿合法慈善機構的官方網站，以竊取毫無戒心的捐助者的錢和/或個人資訊。

州務卿羅伯特·J·羅德里格斯 (Robert J. Rodriguez)

表示，「紐約民眾以支援和慷慨幫助有需要的人而聞名。隨著烏克蘭戰爭的白熱化，騙子將繼續使用情感花招和虛假招攬來欺騙消費者。我鼓勵紐約民眾保護他們的善意，並始終在捐贈之前研究慈善機構，以確保您辛苦賺來的錢能夠用於那些迫切需要您支援的人。」

稅務和財政部代理專員阿曼達·希勒 (Amanda Hiller)

表示，「烏克蘭的全球危機加劇了對網路攻擊的擔憂，因此我們都必須保持警惕，防止機密資訊落入壞人之手、拒絕服務攻擊和其他不良後果。」

資訊技術服務辦公室 (Office of Information Technology Services)

資訊長安吉洛·托尼·李迪克 (Angelo 'Tony' Riddick)

表示，「無數有善心的紐約民眾向慈善機構捐款以支援烏克蘭人民，並且他們正在產生影響。不幸的是，這種慷慨也為網路犯罪分子創造了新的可乘之機。為了保護自己並確保您的慷慨捐贈總能夠到達真正需要幫助的人手中，資訊技術服務辦公室要求紐約民眾遵循這些最佳做法，並對最近的線上威脅和網路詐騙保持警惕。」

國土安全和緊急服務部 (Division of Homeland Security and Emergency Services)

專員傑基·布雷 (Jackie Bray)

表示，「在保護個人資訊和保護自己免受網路威脅方面，每個紐約民眾都可以發揮作用。我們知道，在需要的時候，壞人會在外面尋求欺騙那些試圖提供幫助的人。如果您試圖透過線上或數位捐贈來支援烏克蘭人民，請保持警惕並遵循這些最佳做法，以確保您的捐贈是真實的，並且您的資訊是安全的。」

州參議員凱文·托馬斯 (Kevin Thomas)

表示，「許多紐約民眾採取行動幫助烏克蘭人民，這充分說明了我們的鄰居是有善心的。不幸的是，這也為詐騙者利用這場危機謀取私利創造了絕佳機會。我敦促紐約民眾保持警惕並採取更多的預防措施，確保他們的慷慨捐款用於合法事業。」

議員奈利·洛西奇 (Nily Rozic)

表示，「詐騙者一直在嘗試新方法來進行欺騙，即使在國際危機期間也不會停止。在紐約民眾在烏克蘭人需要的時候齊心協力支援烏克蘭時，至關重要的是，消費者必須掌握確保他們的慷慨不被欺騙的技能和知識。我感謝霍楚爾州長確保紐約民眾不會因為他們的善意而被騙。」

詐騙者經常透過社交媒體、不請自來的電子郵件、電話或簡訊進行聯絡。他們可能會要求使用 Cash App、Venmo 或 Zelle 等支付應用程式匯款，將錢匯到離岸銀行賬戶，或贈送預付禮品卡。最近的許多騙局包括請求以比特幣 (Bitcoin) 或以太坊 (Ethereum) 等加密貨幣進行捐款。騙子很有創意，會不斷想出新的方法來騙人，所以消費者一定要時刻保持警惕。

為防止捐款落入壞人之手，紐約州消費者保護部 (New York State Division of Consumer Protection) 建議採取以下預防措施：

- **驗證請求。** 詐騙者更頻繁地在社交媒體上冒充朋友、家人或戀人並要求捐款；複製他人的照片和傳記資訊並建立線上虛假賬戶很容易。如果您在網上收到不請自來的捐款救濟請求，即使看起來是您認識的人，也請透過不同的通訊連結直接與該人

聯絡以驗證請求。請勿不驗證來源而按任何連結或填寫表單。如果請求來自您最近才在線上認識的人，則很可能是騙局，您應該特別小心。

- **研究慈善機構。**不要只依賴慈善網站。在向任何慈善機構捐款之前，請使用團體名稱以及「評論」和「騙局」等搜尋詞進行線上搜尋。聯邦貿易委員會 (Federal Trade Commission) 建議查詢 give.org、charitynavigator.org、charitywatch.org 或 candid.org 瞭解慈善機構的報告與評分。您還可以向美國國稅局 (Internal Revenue Service, IRS) 核實慈善機構是否已註冊。總檢察長辦公室 (Office of the Attorney General) 還建議在捐贈之前查看[慈善機構登記處](#)的財務報告，以確保慈善機構的財務狀況良好。
- **扛住高壓戰術。**儘管情況緊急，但消費者應扛住立即捐款的壓力。詐騙者經常迫使您立即捐款，導致您忽視他們故事中的危險訊號。當心來自「受害者」和募捐人的直接電子郵件，他們使用令人心痛的故事堅持要您立即捐款。不要透過電話給不請自來的電話推銷員錢；相反，如果您願意，請讓來電者發送有關慈善機構和捐贈地點的書面材料。
- **保護個人資訊的私密性。**切勿在回復不請自來的慈善請求時提供您的社會保險號、信用卡或借記卡號或其他個人身份資訊。如果線上捐贈，請確保您的網際網路連接安全，然後再執行捐贈請求。
- **詢問將如何使用您的錢。**消費者想知道他們的錢直接流向了受害者。真正的慈善機構應該能夠讓您知道您的捐款中有多少將直接用於該計劃，而不是用於管理費用。
- **透過支票或信用卡捐款。**切勿使用現金、禮品卡、加密貨幣或任何難以追蹤的提供物進行捐款。透過支票或信用卡捐款，以確保您有捐款記錄。將支票交給慈善機構，不要交給個人。如果您選擇透過慈善機構的網站捐款，請檢查該網站是否安全以及您的電腦是否配備了最新的防病毒保護。

如果您懷疑遇到了接受捐款的欺詐行為，您可以向紐約州消費者保護部提出投訴，網址為 <https://dos.ny.gov/file-consumer-complaint>。

該部門的消費者援助熱線在週一至週五（不包括州假日）上午 8:30 至下午 4:30 提供服務，電話為 1-800-697-1220。您可以在社交媒體 Twitter ([@NYSConsumer](https://twitter.com/NYSConsumer)) 和 Facebook (www.facebook.com/nysconsumer) 上關注消費者保護部來獲取更多資訊和提示。

在國際社會對網路安全的高度關注之際，紐約州稅務和財政部還分享了一系列重要提示，以幫助納稅人在納稅季節和全年保護他們的私人資訊：

警惕要求提供個人資訊的不請自來的電子郵件和電話。切勿在回復未經請求的電子郵件或電話時分享個人資訊，例如您的社會安全號碼。如果電子郵件或電話聲稱來自與您有業

務往來的公司，請直接致電該公司以確認該聯絡人是否合法。詐騙者經常使用與稅收債務相關的恐嚇策略和威脅來讓您分享您的個人和財務資訊。

保護您的行動裝置。盡快應用修補已知漏洞的軟體更新。使用裝置內置的安全功能，例如密碼，並使用加密數據並在裝置丟失或被盜時遠端刪除內容的程式。

謹慎使用 Wi-Fi

熱點。公共無線熱點並不安全，這意味著網路竊賊很容易在您連接時看到您在行動裝置上所做的事情。限制您在公共 Wi-Fi 上的操作，避免登入敏感賬戶。

瞭解您的應用程式。在下載應用程式之前，請徹底查看應用程式的詳細資訊和規格。查看並瞭解每個行動應用程式的隱私權政策。請注意，該應用程式可能會請求存取您的位置和個人資訊。

謹慎對待您在社交媒體上分享的資訊。避免張貼您的出生日期、電話號碼、家庭住址或可以識別您的工作或愛好的圖片。一個原因：此類資訊可用於確定用於重設密碼的安全問題的答案，並使您成為試圖存取您的賬戶和個人資訊的騙子的目標。

使用強密碼。為您的所有賬戶創建不同的密碼。對於密碼，請嘗試使用至少 14 個字元的密碼，這是當前的行業標準。使用字母（大寫和小寫）、數字和符號的組合。考慮使用密碼短語，即使用容易記住的短語的第一個字母來創建難以猜測的複雜密碼。定期更改您的密碼/密碼短語。

改變您的安全問題。不要多個賬戶使用相同的安全問題。選擇無法透過搜尋社交媒體或網際網路來猜到或找到答案的安全問題。

使用兩步驗證存取賬戶。為提高線上賬戶的安全性，請在登入時盡可能要求提供密碼和額外的安全代碼來驗證您的身份。

謹防網路釣魚。不要按來自未知發件人的電子郵件中的連結、下載裡面的文件或打開裡面的附件。僅當您附件是您想要接收的並知道其中的內容時才打開附件，即使您知道發件人也是如此。

請務必定期查看[確保敏感資訊安全](#)的必要步驟。

報告它。如果您是稅務相關身份盜竊的受害者或認為您可能是受害者，請立即提醒我們。我們將跟蹤您的資訊，以幫助保護其隱私性並保護它。造訪稅務部門的[報告欺詐、詐騙和身份盜竊](#)網頁。

稅務部門使用進階加密、防火牆、入侵檢測系統和其他安全措施來保護我們的系統和敏感數據，但納稅人還必須採取積極主動的方法來保護自己的上網安全。

###

可造訪網站 www.governor.ny.gov 瀏覽更多新聞
紐約州 | 州長辦公室 | press.office@exec.ny.gov | 518.474.8418

[退出訂閱](#)