

太极功夫学院： 世界最高级武术赛事中过关斩将取得优异成绩



通过美国武术总会精心挑选,2名太极功夫学院运动员(Justin Benedik 和 Elva Ly)入选美国国家队。他们顽强拼搏甚至从世界顶级专业武术运动员中脱颖而出。在刚刚结束的2021年国际武联(IWUF)武术套路网络大赛(WTVC)上,身披国家队“战袍”的2名太极功夫学院武术健儿共参与4个比赛项目,全部发挥出色,斩获2枚银牌以及2枚铜牌,用优异的成绩展示了他们的实力和风采。

本次大赛是迄今国际武联主办的参赛人数最多的武术套路专项国际赛事,共吸引了来自61个国家和地区的近千名顶级武术套路运动员参赛。各个国家队由30名(男、女各15人)各国顶级运动员组成。大赛共设长拳、刀术、枪术、剑术、棍术、太极拳、太极剑、太极扇、南拳、南刀、南棍11个比赛项目,分12~14岁,15~17岁,18岁以上三个年龄段,参赛选手的视频需通过指定App进行拍摄提交。此外,为彰显大赛的公平性,本次大赛在国际武联官方微信视频号等多个平台全程播出并现场评分。



疫情期间,国际武联近年来的各项赛事和活动延期举办,给广大运动员们的训练和生活造成了不小的影响。今年由国际武联主办的武术套路网络大赛以“线上比武”的形式,为五大洲的优秀运动员们提供了交流和提高的新平台。虽受疫情

影响,但困难是暂时的,我们在共同应对挑战中凝聚信心,传递希望。在祝贺Justin和Elva取得优异成绩的同时,希望太极功夫学院的学员们再接再厉,疫情过后再次代表美国在世界顶级武术赛事中发光发热。

新冠疫情期间诈骗风险依然存在;安全峰会在特别周内聚焦纳税人和税务专业人士,防止身份盗用

华府——随着2022年纳税季节和假期的临近,美国国税局、州税务机构和国家税务行业今天宣布了推出特别周,主题重点为纳税人保护敏感财务信息免受身份窃贼的侵害。

第6届年度国家税务安全意识周将于11月29日至12月3日开展,为安全峰会、美国国税局、各州和国家税务界的联盟计划。本次声明恰逢国际欺诈宣传周结束。

峰会合作伙伴警告说,未来几个月纳税人和税务专业人士将面临更大的风险,因为欺诈者会利用新冠疫情,诱骗人们通过电子邮件、短信和在线泄露敏感个人信息。身份窃贼可以使用该信息来提交纳税申报表和窃取退税。

随着安全峰会合作伙伴加强针对身份盗用的联合防御,包括通过身份盗用信息共享和分析中心(ISAC),欺诈者地寻找获取更为疯狂寻找方法绕过防御,获取敏感个人财务信息。这使得税务专业人士(他们为客户持有有价值的税务信息)成为骗子锁定的目标。

“国家税务界已成功联手通过安全峰会努力保护纳税人,但在这场持续的斗争中需要帮助。”美国国税局局长Chuck Rettig表示,“纳税人和税务专业人士是第一道防线,抵御骗取退税的犯罪分子。我们正在进入一个敏感的假期和纳税期,我们敦促民众保护他们的个人信息,避免在纳税时间出现问题。”

国税局和安全峰会合作伙伴亦注意到层出不穷的安全威胁和骗局。骗子们可以通过虚假电子邮件、短信和线上诈骗来模仿国税局工作人员或别的税务工作者。骗局往往以新冠疫情主题、经济刺激付款或退税为幌子。他们亦经常使用新近发生的悲剧或假扮慈善团体来诱使人们分享敏感的财

务数据。

为了解决这个问题,峰会合作伙伴的国家税务安全意识周将提供为期一周的系列教育材料,以帮助保护个人、企业和税务专业人士免遭身份盗用,包括提供一系列特制的资讯图表,和在社交媒体Twitter和Instagram上通过@IRSnews和#税务安全分享信息。

今年的一个特别关注点是将税收安全意识集中在年轻和年长的美国人身上。一些人即使不提交纳税申报表,他们的在线互动也可能导致骗子获取敏感信息并利用信息获得退税。

美国国税局和安全峰会合作伙伴进一步致力于税务安全的宣传,并在YouTube上分享有关纳税人安全步骤的视频。视频包括通过简单的步骤来保护计算机和电话(英文),采取安全措施防止与税务相关的身份盗(英文),民众可以在线观看或下载这些视频。

出版物4524《纳税人的安全意识》(英文),便于雇主与员工和顾客分享,税务专业人士与客户共享。

今年国家税务安全宣传周的亮点包括:
第1天 - 网络星期一:保护在线个人和财务信息

美国国税局和安全峰会合作伙伴(英文)提醒人们采取以下基本措施:

在电脑和手机上使用安全软件,并保持更新。

避免网络钓鱼诈骗,尤其是与退税和新冠疫情、经济影响付款和其它税法变更相关的诈骗。

为所有帐户使用强大且唯一的密码。尽可能使用多重身份验证。

只在安全网站购物;寻找网址中的“https”和挂锁图标;避免在咖啡店、商场或

餐馆等地方使用不安全的公共Wi-Fi购物。
第2天 - 慈善星期二:提防骗子使用假慈善机构

美国国税局和安全峰会的合作伙伴警告人们在向慈善机构捐款时避免被骗。该机构提供以下提示:

个人不应该让任何来电者强迫他们捐赠,捐赠前请务必花时间做好研究和调查。

询问受捐赠对象的确切名称、网站和邮寄地址并稍后确认,确认该慈善机构是真实的。

注意捐赠的方式。在研究了慈善机构后,用信用卡或支票支付,而不是用礼品卡或电汇。

第3天 - 获取身份保护个人识别号码
纳税人如果可以在线验证身份,则请选择加入国税局个人身份识别号码(IP PIN)计划。该计划是前几年的一项重大扩展。这是纳税人可以用来保护自己退税的另一种工具。以下是纳税人需要知道的:

身份保护PIN或IP PIN是一个只有个人和国税局知道的六位代码。它为纳税人在纳税申报表上的社会安全号码提供了另一层保护。

使用IRS.gov/IPPIN上的获取身份保护PIN(IP PIN)工具立即获取IP PIN。

切勿与任何人共享IP PIN,除非是可信的代报税人。

第4天 - 税务专业人士应审查他们的安全协议

身份窃贼一直以税务专业人士为目标,美国国税局和峰会合作伙伴敦促从业者审查“税收-安全-共同”清单,其中包括:

采取基本的安全措施。

使用多重身份验证来保护税务软件帐户。

根据联邦法律的要求制定书面数据安全计划。

了解网络钓鱼和电话诈骗,尤其是与电子归档识别号(EFIN)、新冠疫情相关税法变更(包括经济影响补助金的付款)相关的诈骗。

创建数据安全和数据盗窃恢复计划。

第5天 - 使用数字签名提交国税局表格并在安全门户上检查帐户详细信息

去年,美国国税局开始接受各种形式的数字签名。此外,国税局还改进了其在线帐户平台,以更好地服务于税务专业人士和个人。

税务专业人士可以前往IRS.gov上的新税务专业账户以数字方式发起委托书和税务信息授权请求。

纳税人可以在线控制谁可以代表他们或在在线门户上查看他们的帐户信息。美国国税局现在接受多种无法以电子方式提交的表格上的数字签名。

第6天——企业应实施保障措施,提防与税务相关的骗局

大多数网络攻击都针对员工少于100人的小型企业。以下是该部分的一些详细信息:

了解小型企业的最佳安全实践。

国税局会一直保护性屏蔽业务记录中的敏感信息。

企业身份盗窃宣誓书《14039-B表》可供所有企业向国税局报告盗窃行为。

谨防各种骗局,尤其是试图窃取员工收入信息的W-2骗局。

在IRS.gov/identify theft上查看国税局身份盗窃中心的“企业”部分。

如果远程工作,则创建一个虚拟专用网