公共服务公告

联邦调查局

警报编号： I-010324-PSA

2024 年 1 月 3 日

中国假冒警察采用激进手段瞄准美国华人社区

美国联邦调查局 (FBI) 警告公众，冒充中国警察的犯罪分子正瞄准美国的华人社区进行诈骗，尤其是针对在美国大学就读的中国学生。 犯罪分子会告知受害者，他们因涉嫌在中国进行金融犯罪而接受调查，需要付钱以避免被捕。犯罪分子之后会引导受害者同意全天候视频和音频监控。该骗局包括四个阶段。

第一阶段 - 初次接触：冒充美国企业或中国大使馆/领事馆人员

犯罪分子打电话给受害者，典型的做法是用科技手段来掩盖或篡改他们的真实电话号码，让电话看似来自移动电话服务提供商，大型零售商、送货服务或中国大使馆/领事馆。犯罪分子告诉受害者他们因个人身份信息与金融欺诈的嫌疑人或受害者相关联而被调查。

第二阶段 - 恐吓战术：冒充中国警察

犯罪分子据称会随后将电话转接到正在办理此案的中国省级公安局。一名冒充中国警察的犯罪分子藉此向受害者提供涉案细节并提供虚假文件，例如所谓的执法证件、受害者的中国身份证照片和其他涉嫌指控罪名的文件。犯罪分子会给受害者施压让他们返回中国接受审判，或以逮捕相威胁。

第三阶段 - 监控受害者

因为调查的敏感性或用以证明受害者的清白，犯罪分子会引导受害者同意全天候视频和音频监控，指示受害者不与他人讨论案件细节，不进行互联网搜索，并报告他们的所有日常活动。

第四阶段 - 最后一步：勒索受害者

犯罪分子指使受害者向中国境内银行账户汇入大额资金来证明其无罪或获得保释以避免返回中国。在有些情况下，犯罪分子会让受害者向朋友和家人撒谎来获得额外资金，让他们充当钱骡或协助诈骗其他的在美就读学生。

防骗小常识：

- 如果一个身份不明的人与您联系，指控您犯了罪，请不要泄露任何个人身份或财务信息，不要进行任何汇款，停止与此人的任何进一步接触。
- 看似来自官方号码的电话不代表就是官方电话。犯罪分子可能会使用科技手段来伪装或篡改他们的实际号码，让来电号码看似可信。
- 如果任何政府机构出于所谓的官方目的与您联系，您可以使用公共资源（电话簿，互联网等）来查询政府机构的联系信息，对其官方身份进行验证，然后直接与该机构联系以确认联系是否属实。
- 不要同意全天候视频或音频监控。
- 如果您觉得有自称是中国当局的个人与您联系， 请联系您当地的联邦调查局分局。外国政府在美国进行合法执法活动的官员必须与美国联邦当局协调行动。

举报：

联邦调查局要求受害者登录 FBI 互联网犯罪投诉中心网站 www.ic3.gov，在第一时间举报此类欺诈或可疑活动。请确保在举报中包含尽可能多的交易信息，例如电汇说明、钱包地址、电话号码，以及短信或电子邮件内容。

此外，联邦调查局建议采取以下措施：

- 向交易使用的支付服务提供商举报。
- 立即联系您的金融机构来阻止或撤销此次交易，并让金融机构联系资金转入的相关金融机构。
- 向您的校园安全或公共安全办公室举报，以提高学生群体安全意识。
- 犯罪分子可能会使用类似的手段来欺诈华人社区的其他成员，而不只限于在美就读的中国学生。

有关类似诈骗或欺诈活动的更多信息，请参阅之前的公共服务公告:

IC3 | Criminals Pose as Chinese Authorities to Target US-based Chinese Community

IC3 | 繁體中文版 (in Chinese – Traditional Written)

IC3 | 简体中文版 (in Chinese - Simplified Written)