国家反诈中心　外交部领事保护中心　教育部留学服务中心
Chinese Service Center for Scholarly Exchange

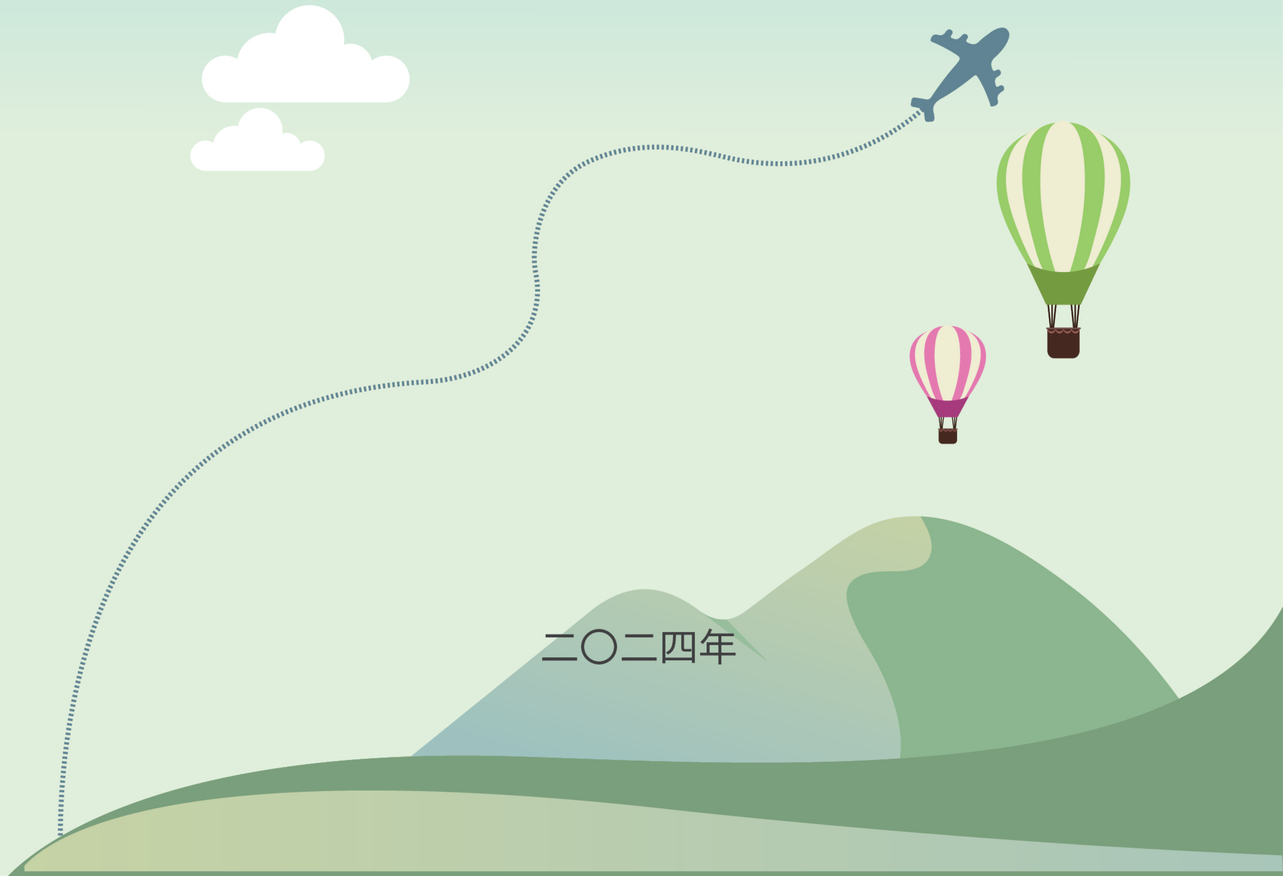
国家反诈中心　外交部领事保护中心　教育部留学服务中心
Chinese Service Center for Scholarly Exchange

海外防范电信网络诈骗

OVERSEAS PREVENTION OF TELECOM ON-LINE FRAUD

宣传手册

Brochure



目录 CATALOGUE

01 牢记六个凡是

牢记六个凡是 01

02 海外高发案件类型

（一）冒充公检法类诈骗 02

（二）虚拟绑架类诈骗 04

（三）虚假网络投资理财类诈骗 06

（四）虚假服务类诈骗 08

（五）虚假换汇类诈骗 10

（六）冒充熟人类诈骗 12

（七）企业邮箱类诈骗 14

（八）海外高薪招聘骗局 16

03 诈骗手段新动向

（一）谨防“二次诈骗” 17

（二）勿当诈骗“工具人” 17

04 反诈利器

（一）国家反诈中心APP 18

（二）官方政务号 18

牢记6个凡是

1. 凡是自称驻外使领馆、运营商、海关等工作人员，以涉嫌相关违法犯罪为由，主动将电话转接至公安机关的，都是诈骗！
2. 凡是自称公检法工作人员，要求你拍摄被绑架的照片、视频，或是要求缴纳高额取保候审金、将资金转入“安全账户”的，都是诈骗！
3. 凡是宣称“内幕消息、专家指导、稳赚不赔、高额回报”的投资理财，都是诈骗！
4. 凡是打着低价换汇名义，要求先行转账的，务必提高警惕，谨防被骗！
5. 凡是自称驻外使领馆工作人员向你推荐指定机构，声称可以包办护照、签证等手续的，务必提高警惕，谨防被骗！
6. 凡是自称“熟人”主动在社交平台添加好友，请你帮忙代购机票、支付购物尾款的，务必提高警惕，谨防被骗！

（一）冒充公检法类诈骗

诈骗套路

前期引流

1、自称“运营商或银行客服”：“您名下的电话卡/银行卡涉及案件，需要配合调查”。

2、自称“驻外使领馆工作人员”：“您因非法滞留/签证无效，需要配合警方调查，否则将被遣返回国”。

3、自称“物流公司客服”：“您的包裹被海关拦截，因内藏毒品/大量银行卡，需要接受调查”。

诈骗分子冒充电信运营商或银行客服、驻外使领馆工作人员、物流公司客服等身份与受害人联系，以涉嫌洗钱、贪腐、银行卡涉案、冒用身份等理由，要求受害人配合调查，并将电话转接至国内“公安机关”。

威胁恐吓

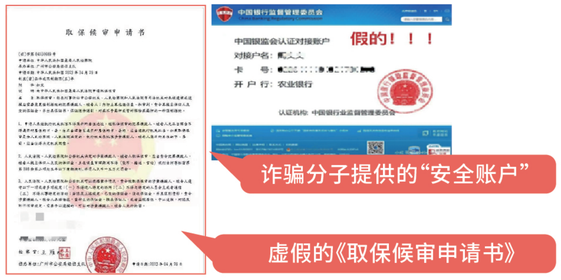
电话转接至“公安机关”后，诈骗分子扮演的“假警察”为了获取信任，通常会转移到指定聊天软件向受害人出示案件受理书、通缉令、警官证等，甚至身着假警服、在伪造的公安机关办案场景下与受害人进行视频通话，还会要求受害人签订保密书、定时汇报个人动态，进一步对受害人进行精神控制。


虚假案件回执单

虚假通缉令

诈骗分子正在与受害人进行视频通话

骗取钱财



诈骗分子提供的“安全账户”

虚假的《取保候审申请书》

方式一：以资金核查为由，要求受害人提供银行卡号、密码、验证码等信息，直接完成盗刷；或让受害人将所有资金转入“安全账户”，承诺核查完毕后将资金原路返还。

方式二：向受害人出示虚假的取保候审申请书，要求受害人缴纳高额保证金，并声称如不缴纳将被羁押、遣返回国等，以此骗取钱财。

典型案例

在海外留学的孙某接到一个电话，对方声称孙某名下的手机号码向多位用户发送了诈骗短信，由于该涉诈号码的注册地在上海，如需证明不是孙某本人行为，需要向上海市公安局申请调查。随后，对方将电话转接至“上海市公安局”的“李警官”，声称孙某还涉嫌跨国非法洗钱犯罪，需要签订“保密协议”，并要求下载SKYPE视频通话软件，每隔三个小时报告一次个人情况。“李警官”告知孙某可以向“检察官”申请“优先调查”，同时必须缴纳足额的保证金才能予以取保候审，否则可能会被引渡回国。孙某因担心学业受到影响，于是根据“检察官”的指引，先后两次将共计43000美元转到对方指定的资金账户。转账后，孙某再也没有收到对方的消息，遂发觉被骗。

如何识破骗局？

1、公检法等国家机关不存在电话转接。凡是自称“驻外使领馆、电信运营商、银行”等工作人员，并主动帮忙转接到公检法等国家机关的都是诈骗。

2、公检法等国家机关不会向受害人在线发送“通缉令”“逮捕证”“取保候审决定书”等法律文书。

3、公检法等国家机关不存在“安全账户”。凡是以配合调查为由，要求“将资金转入安全账户进行资金核查”或是“缴纳高额取保候审金”的都是诈骗。

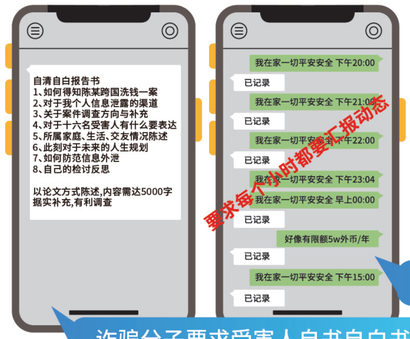
防骗提示

如遇“国家机关工作人员”主动联系，应及时与当地相关部门进行核实。公检法等国家机关内部有规范的工作流程及严格的保密要求，不会通过微信、QQ以及Telegram等境外聊天软件发送逮捕证等法律文书，更没有“安全账户”，凡是要求转账进行资金核查的都是诈骗！

（二）虚拟绑架类诈骗

诈骗套路

诱导控制

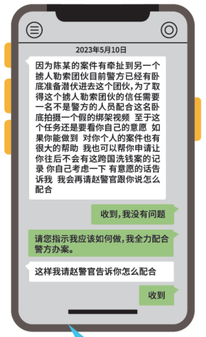


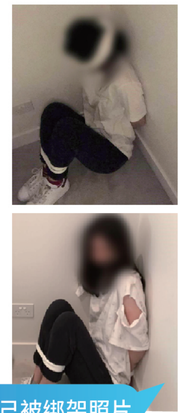
诈骗分子要求受害人自书自白书

诈骗分子要求受害人定时汇报个人动态

诈骗分子冒充公检法机关工作人员致电受害人，谎称其涉嫌重大犯罪，要求受害人“配合调查”迫使其离开居住地，前往宾馆或其他国家，并要求切断手机、微信等与家人或亲友取得联系的渠道，还会要求受害人自书“个人情况自白书”、定时汇报行程及个人状态，以对其进行精神控制。

伪造绑架



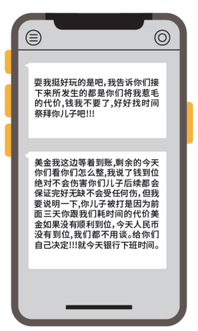


诈骗分子以配合警方卧底为由诱导受害人“虚拟绑架”

受害人拍摄自己被绑架照片

诈骗分子引导受害人拍摄被绑架的照片、视频。以受害人曾自导自演“绑架案”逃避侦查为由，要求其拍摄视频作为对比以自证清白。或是当受害人无法按照要求缴纳巨额保证金时，诈骗分子声称让受害人伪造被绑架的假象，以向其家人索取资金。或是声称受害人本人或父母涉嫌重大案件，若其配合拍摄照片、视频，配合警方完成秘密任务，即可获得宽大处理。

骗取“赎金”



诈骗分子引导受害人向其家长谎称孩子被“绑架”，并发送事先拍摄好的照片或视频以证明“绑架”真实性，向家长骗取巨额“赎金”。

典型案例

在海外某国留学的李某接到了自称“国内移民局工作人员”的电话，称其在广州白云机场有异常出行记录，即将被机场公安追究责任。其后，又有三名自称广州警方的男子先后与她通话，称其涉嫌参与跨国洗钱活动将被遣送出境。对方要求李某登录一个所谓的“公安部”网站自行查询，李某输入案件查询编号后，发现上面竟然有自己的“通缉令”。随后，对方又称怀疑李某自导自演了一场“绑架案”以逃避调查，要求她拍摄视频来自证清白。根据诈骗分子的要求，李某自行拍摄了被绑架的求救视频提供给“警方”进行声话比对真假，并提供了自己的微信账号及密码。诈骗分子谎称即将有执法人员来抓李某，让其出境避难，同时，使用李某微信号联系其父母，利用其拍摄的视频假称李某被绑架，索要赎金500万元。

如何识破骗局？

1、公安机关在办理案件时不会要求签订所谓的“保密书”，更不会要求受害人自编自演“绑架案”。

2、公安机关不会线上办案，不会使用屏幕共享软件，更不会要求使用境外社交软件定时汇报个人动态。

防骗提示

如接到声称“警方办案”“协助调查”等可疑电话，切勿轻易相信，及时通过官方渠道联系中国驻当地使领馆，或向所在学校老师、同学、警方核实求助，并及时告知家长相关情况。留学生家长如接到可疑电话声称子女被绑架，应当立即报警，切勿轻易转账汇款。

（三）虚假网络投资理财类诈骗

诈骗套路

获取信任

受害人会被拉入所谓的“投资”群聊，诈骗分子冒充投资导师、金融理财顾问，多以投资虚拟币、区块链等高科技产品为名，在群中开“直播课”或发送投资成功的假消息以骗取受害人信任。或是诈骗分子通过婚恋交友平台先与受害人谈感情，确定婚恋关系，再以有特殊资源、平台有漏洞、可获得高额理财回报等理由，骗取受害人信任，引诱其进行投资。

诈骗分子安排托儿在群中吹捧“导师”，制造假象

虚假投资群中诈骗分子分享“投资经验”

诱导投资

诈骗分子委托受害人代为管理虚假投资平台账号，按照“导师”指令进行操作，诈骗分子通过修改后台数据，向受害人分享虚假提现截图，引诱受害人开设账户进行投资。

拉黑消失

受害人前期小额投资试水一般会获得返利，但一旦加大资金投入，就会出现无法提现的情况，诈骗分子会再以缴纳保证金、个人所得税、解冻金等理由继续诱导转账，受害人最终会在转出大量资金后被踢出群聊并拉黑。

诱导受害人借钱投资

诱导受害人缴纳高额的个人所得税

典型案例

海外中国公民王某在Instagram上认识了网友何某，双方相谈甚欢，后在WhatsApp互加好友。而后何某开始与王某讨论加密货币交易，声称要带王某赚钱。在何某的诱导下，王某开始使用Trust钱包在何某提供的投资网站进行投资。王某将其所有积蓄全部投入后，何某又诱导其贷款、向家人朋友借钱进行投资。王某先后在该网站投资12笔共计30万人民币，交易平台显示盈利。随后，王某尝试提现，被客服告知需要先缴纳20万元的税款，王某无奈继续编造理由向家里借钱。缴纳税款后，客服称提现时被系统风控，需要再缴纳10万，王某借遍了亲朋好友的钱凑齐并缴纳保证金后，网友何某与平台客服一并失联，王某所投资钱款“不翼而飞”。

如何识破骗局？

1、虚假投资理财类诈骗APP无法在正规应用市场检索到，诈骗分子会引导受害人通过扫描二维码或点击网址链接下载安装APP。

2、虚假投资理财平台大多会要求受害人将资金转账到指定的个人账户或者名称与当前平台不符的对公账户。

3、网络上素未谋面的“理财大师”“投资导师”“网恋对象”向你推荐投资理财时要保持高度警惕。

防骗提示

不要轻信非正规渠道推荐的投资理财。

凡是标榜“内幕消息”“稳定高回报”的网络投资理财，都是诈骗！

（四）虚假服务类诈骗

诈骗套路

前期引流

诈骗分子在群内发布虚假租房广告

诈骗分子伪装成驻外使领馆工作人员、房东或中介、培训机构工作人员等身份，在网络社交工具、网页、搜索引擎等渠道发布广告，以可提供办理签证、租房、升学、代写论文等服务为诱饵，吸引有需求的群体并建立联系。

获取信任

诈骗分子伪造虚假资质证明、房产证明等文件，使受害人相信其可以提供帮助升学、办理签证、租房等服务。

伪造虚假资质证明
获取信任

实施诈骗

受害人交纳服务费后，却未能得到相应服务，待与对方再次联系时，发现已被拉黑，或是对方以其他理由继续诱导受害人转账。

典型案例

海外留学生张某在社交平台上看到一套合适的出租房，位置临近大学且价格偏低，张某生怕错过了好房源，随即心急火燎地联系“房东”。“房东”表示自己是华人，并向其发送了一段房屋视频。张某觉得房屋各方面的条件都很不错，于是按照“房东”的要求交纳了三个月的租金作为定金。随后“房东”以需要签订房屋租赁合同、交纳中介费等为由，一次又一次地推迟交房时间。最后在张某提出退租要求时，“房东”突然联系不上了，张某才发现被骗。

如何识破骗局？

1、诈骗分子通常只在线上沟通，对见面交易总以各种理由推脱。

2、诈骗分子往往以“交纳中介费”“交纳服务费”“签订合同”等理由推迟交付或不提供相应服务。

防骗提示

一定要选择正规的购物、服务平台，对异常低价的商品务必提高警惕。租房要通过正规中介，签订合同前应认真查看核实中介资质，通过线上线下方式综合判断房东或中介的真实性、合法性，通过房产登记机构核对房屋产权归属和房屋情况等信息，谨防被骗。

（五）虚假换汇类诈骗

诈骗套路

前期引流

诈骗分子通过网络社交工具、网页、搜索引擎等渠道发布广告，披着低价、合法、正规等外衣，声称可以提供换汇服务。

建立信任

诈骗分子向受害人展示伪造的好评截图、资质证明等虚假材料，并通过前期小额成功换汇，以获取受害人信任，后与受害人商定交易汇率，确定交易方式。

实施诈骗

诈骗分子声称已将换汇资金转入受害人账户，要求其将待换汇资金转至指定账户。若受害人发现实际没有收到转账，诈骗分子便会发送伪造的银行汇款记录、支票、转账记录等虚假支付凭证，以跨行转账延迟等理由推脱，催促受害人尽快转账，完成诈骗。

典型案例（一）

海外留学生张某因日常开销需要，打算用人民币兑换一些美元。张某从朋友圈里看到有“朋友”发布提供换汇服务广告，且汇率很有吸引力，于是与其联系，双方确定了换汇金额。随后对方给张某发来一张向其银行账户汇入1万美元的交易截图，并催促张某尽快转账，张某见状便将相应人民币通过微信转账支付给对方。但张某却迟迟没有收到美元，再联系“朋友”时发现已被对方拉黑，才发觉被骗。

典型案例（二）

诈骗分子操控两名有相反换汇需求受害人进行线下交易，要求其中一人A提前通过网上银行进行转账，承诺可线下取现，并要求另外一人B线下直接换汇。在线下交易过程中，B将现金给A后，A因已把钱款线上转账给骗子，拒绝向B提供现金，二人因此产生纠纷，发现被骗。

防骗提示

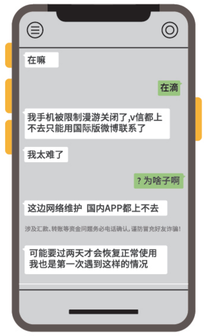
诈骗分子往往会发布优惠换汇信息吸引受害人，当汇率大幅偏离市场价时，务必提高警惕。

私下换汇有风险，很可能无形中成为了犯罪分子的洗钱工具，从而导致法律风险。

（六）冒充熟人类诈骗

诈骗套路

获取信任



诈骗分子使用受害人家人、朋友的照片、昵称包装社交账号，添加受害人为好友，以冒用的身份对受害人嘘寒问暖表示关心，从而骗取受害人信任。

诈骗分子制作高仿账号添加受害人

提出需求

诈骗分子编造理由向受害人求助，一般以自己账号出现问题无法购买机票、无法支付购物尾款、有急事需要用钱等理由，要求受害人帮其支付或转账。

诈骗分子谎称支付出现问题

骗取钱财

诈骗分子会以时间紧迫、事情重要等理由催促受害人尽快转账，待受害人转账支付后，便将受害人拉黑失联，完成诈骗。

诈骗分子完成诈骗后将受害人拉黑

典型案例

张某收到一条社交平台私信，对方声称是其在国外留学的女儿，因为微信登录不上，所以通过该社交平台与她联系。随后，张某在微信上给女儿发了一条信息，但其女儿迟迟未回复消息，张某便相信了该社交平台上与其联系的是自己女儿。“女儿”告诉她，学校有一位同学已返回中国，该同学在回国前给了她2万英镑，请她帮忙把英镑换成人民币，而她换了钱后因登录不了微信所以无法把钱转给同学。于是张某便根据“女儿”指引，直接添加了其同学的微信，替“女儿”先行转账9万元给这位同学。直到张某的真女儿在微信上给其回复消息，她才发现被骗。

如何识破骗局？

1、诈骗分子一般会制作高仿账号与受害人进行联系，当遇到相同昵称、头像的“熟人”添加好友与你联系时，务必保持警惕。

2、当受害人提出通过语音或视频通话进行确认时，诈骗分子通常以不方便接电话等理由拒绝，或短暂接听几秒钟后迅速挂断。

3、诈骗分子通常会以购买机票、急需付尾款等紧急情况为由，不断催促受害人转账。

防骗提示

凡是接到自称家人、熟人要求转账的信息时，务必通过打电话、开视频等方式向熟悉情况的人核实，在确认之前切勿转账！

（七）企业邮箱类诈骗

诈骗套路

盗取邮箱

诈骗分子通过植入木马等手段，盗取企业邮箱的用户名和密码，通过跟踪和偷窥邮箱内的邮件，深入了解企业和合作伙伴之间的生意进程，掌握双方的交流习惯和业务细节。

潜伏观察

在深入了解双方生意进程的同时，诈骗分子会提前注册好与收款企业邮箱地址相似的“虚假邮箱”，时刻关注双方发生交易的时间点，冒充收款方与汇款方进行沟通。

实施诈骗

诈骗分子使用“虚假邮箱”向汇款方发送邮件，称因自己的收款渠道出现问题或公司内部调整等原因需要变更收款账户，并将诈骗分子的账户发送给付款方，骗取货款。

典型案例

A公司定期从B公司购买货物，双方通过邮箱约定近期进行交易，但是A公司的企业邮箱收到自称B公司ny****@neva.com(B公司真实电子邮箱为ny****@nave.com，两个电子邮箱地址高度相似)发来的新订单，称近期因银行方面出现问题，此次交易的货款需支付到新的收款账户。A公司未进行核实便将587440欧元货款支付到新账户，之后发现被骗。

如何识破骗局？

生意往来过程中，如对方邮箱地址或银行账户发生变动，务必要与前期留存记录比对，进行各方核实，切勿轻易转账。

防骗提示

企业与合作伙伴都应当增强安全意识，当交易信息突然发生变动时，务必验证核实，以确保交易资金安全。

（八）海外高薪招聘骗局

诈骗套路

诈骗分子以工作简单、月入过万、稳赚不赔、包吃包住、报销机票、专人接送等信息为诱饵，在邮箱、贴吧等互联网渠道发布海外高薪招聘广告，诱导急需找工作的公民通过非法途径到境外，而后以采取限制人身自由等方式强迫其从事电信网络诈骗等违法犯罪活动，危害公民的人身及财产安全。

防骗提示

1、在找工作时，要对招聘信息多加甄别，切勿轻信所谓“门槛低、工资高”的海外高薪招聘信息，更不要以非法途径前往境外，避免落入犯罪团伙的陷阱。

2、如在海外人身安全受到威胁，应及时向警方求助。报案信息应尽可能详细提供，以帮助警方提高成功解救机率。

（一）谨防“二次诈骗”

诈骗套路

诈骗分子利用已被骗的受害人易于上当、止损心切等特点再次施骗。假扮网警、律师等身份，以回款为诱饵，称可在网络上帮助受害人立案调查，或通过起诉已转账银行等方式维权追回钱款，再次骗取受害人钱财。

防骗提示

切勿相信陌生来电或网络上假冒的“警察”“律师”可以追回钱款等说辞，谨防被“二次诈骗”。

（二）勿当诈骗“工具人”

诈骗套路

诈骗分子冒充公检法机关工作人员对受害人实施诈骗后，对该受害人进一步控制，使其在不知情的情况下成为诈骗分子的“帮凶”，利用该受害人在当地开展针对其他受害人的诈骗活动。诈骗分子通常声称如配合开展工作便可获得“取保候审”“戴罪立功”机会，并“聘任”受害人为“辅警”，要求受害人配合“国内警方”在当地开展工作，比如对其他受害人实施“秘密抓捕”“签订保密协议”“讯问”等，以便诈骗分子进一步实施诈骗活动。

防骗提示

公检法机关不会委托海外中国公民开展抓捕犯罪嫌疑人、讯问、签订保密协议书等执法工作，更不会要求海外中国公民实施危害他人人身安全的行为，如遇此类情况，切勿轻易相信。

（一）国家反诈中心APP

国家反诈中心APP是一款官方手机防骗保护软件，集诈骗预警提示、报案助手、线索举报、反诈宣传等多种功能于一体，可以有效提升用户的识骗防骗能力。

国家反诈中心 APP
Android 下载

国家反诈中心 APP
ios 下载

（二）官方政务号

国家反诈中心、外交部领事保护中心、教育部留学服务中心开通官方政务号，全面解析高发诈骗类型，宣介海外反诈常识，发布海外防诈提醒，欢迎关注。

国家反诈中心
微信视频号

国家反诈中心
微博号

国家反诈中心
抖音号

国家反诈中心
快手号

外交部领事直通车
微信公众号

外交部领事直通车
微博号

外交部领事直通车
抖音号

外交部领事直通车
快手号

外交部领事直通车
哔哩哔哩号

教育部平安留学
微信公众号

教育部平安留学
网站