

近

年来，国际电信网络诈骗案件频发，其中最为典型的骗术是冒充中国驻外使领馆或中国公检法人员实施诈骗。某天，旅法中国公民（留学生）张伟接到了这样一通电话：



“吴主任”

张伟，你好！这里是中国驻法国大使馆，我是领侨处吴主任，您有一份重要文件在使馆待领取，请尽快来使馆领侨处领取。

需要现在就过来吗？这真的是使馆的电话吗？



张伟



“吴主任”

你这都不信？你可以查一下使馆网站，看是不是使馆电话？这件事很着急，我直接告诉你吧，A市警方昨天给使馆发了一份传真，告知你涉嫌一起重大刑事案件，我可以把电话转到A市公安局“贾警官”，你们可以直接联系。

（张伟上网查询后发现，来电显示确为使馆公布的办公电话，于是放松了警惕，殊不知不法分子可以使用技术手段将来电显示篡改为任何号码。随后，电话被“转接”至A市公安局“贾警官”。）



“贾警官”

我们近日在机场抓获一名涉嫌特大跨国洗钱案件的嫌疑犯，他身上有一张你名下的银行卡，请配合我们进行调查，这也是每位公民的法定义务。

可我名下没有这张银行卡。



张伟



“贾警官”

那可能是你的身份信息被嫌疑人盗用了，但我们还不能完全排除你的涉案嫌疑，请尽快到我局接受调查。

可我现在不在国内啊。



张伟



“贾警官”

如你不方便来我局，也可以通过某软件远程办案。这件事很严重，如你拒不配合，我们将联系国际刑警组织将你列入通缉名单，要求法国警方吊销你的居留卡并对你实施遣返。

（张伟有些害怕，按对方要求下载了某软件，与“贾警官”互加好友并视频通话。镜头里的“贾警官”身着警服，正襟危坐，背景上有“A市公安局”等字样，殊不知，这是犯罪分子精心布置的“现场”和“道具”，目的是进一步坐实自己的公职人员身份，从而骗取张伟的绝对信任。）



“贾警官”

我很严肃地告诉你，因为犯罪分子用你名下这张卡诈骗，已经导致数千名群众上当，还有多名受害者自杀。犯罪分子在口供中明确说你是他们的同伙，警方已对你签发了逮捕令，看看这是不是你的身份证，所以你要完全配合警方调查。你现在就要安装某远程监控软件，从现在开始每六个小时向我报备行踪并接受远程视频检查。这是国家二级保密案件，你必须删除微博和小红书，不要和其他人谈及案情，也不能联系使馆。

（张伟定睛一看，视频中“贾警官”出具的确实是自己的身份证，“逮捕令”上还盖有“A市公安局”的红色印章。至此，张伟彻底相信了“贾警官”的身份，按照“贾警官”要求，在接下

来两周里，他每天进行四次所谓的“安全汇报”，并陆续提供了自己的大量个人信息。）



“贾警官”

张伟，警方对你的调查已基本结束，可以判定你是无辜的，接下来要进行资金清查，需要你缴纳50万元人民币申请保释，请汇款至警方指定的“安全账户”，法院正式宣判后如果你无罪，这笔钱会原封不动退还给你。

可我手头没有这么多钱。



张伟



“贾警官”

这不是警方要考虑的问题，你可以找朋友借也可以向家长要，关键是在规定时间内汇款，这对你申请保释很重要，否则警方会认为你不配合办案且有潜逃嫌疑。

（张伟始终对“贾警官”的身份深信不疑，多方筹措50万元人民币汇到犯罪分子指定账户，“贾警官”至此也销声匿迹。）

通过模拟上述电信诈骗典型场景，中国驻法国使领馆再次郑重提醒旅法中国公民，尤其是旅法中国留学生：中国驻外使领馆和中国公检法机关有严格工作程序，不会通过电话告知您“涉案”，更不会通过社交软件“办案”；不会将电话转接至所谓“公安局”“检察院”或“国际刑警中心”；不会要求进行“安全汇报”或以“案件涉密”为由要求切断与家人联系；不会索要银行账户信息、要求缴纳“保释金”或将资金转移至“安全账户”。接到此类电话，您只要做到不紧张、不轻信、不转账，直接挂断电话即可。

如出现个人信息泄露，请立即切断与不法分子联系。如已汇款，请尽快联系银行冻结资金。如已造成损失，请同时向法国警方和国内公安机关（可拨打110或96110转反诈中心）报案。

防范电信网络诈骗活页



中国驻法国大使馆
AMBASSADE DE CHINE
EN FRANCE



微信公众号



领侨处小红书号

警惕身边的陷阱

电信网络诈骗典型案例

1. 冒充快递员实施的诈骗

林先生收到一名自称“快递员”的短信 (Est-ce que vous êtes chez vous?), 表示林有一个包裹投递失败, 需缴纳滞纳金并重新预约投递时间。“快递员”还“贴心”发来预约链接, 林先生打开该链接并按要求填写银行卡信息后, 银行卡遭到盗刷。

2. 冒充移民局等政府机构实施的诈骗

邓先生接到自称“法国移民局”工作人员来电, 表示接到电信运营商投诉, 邓先生名下手机号近期发送大量垃圾短信, 怀疑其涉嫌诈骗, 要求邓先生配合调查, 否则将取消其居留并实施遣返。邓先生表示自己从未从事上述行为, 对方表示可以申诉并通过短信发来链接。邓先生点击后, 浏览器提醒系伪造政府部门网站, 邓先生随即中止与此人联系。



3. 冒充微信和银行客服实施的诈骗

王女士接到自称“微信安全中心”工作人员来电, 表示其微信钱包收付款异常, 需将电话转接至银行“客服人员”解决。“客服人员”表示因王女士的个人信息遭泄露, 导致微信钱包出现安全风险, 需提供银行卡卡号、密码和短信验证码进行“安全加固”。王女士按“客服人员”进行操作, 卡内资金被不法分子转走。

4. “杀猪盘”类型诈骗

陈同学在某社交媒体上结识了同在国外留学的张同学, 两人迅速发展成“网恋”关系。某日, 张同学联系陈同学称, 自己在外省实习期间遭遇车祸, 希陈同学为其垫付5000欧元手术费。在查询网上有关案例并与家人沟通后, 陈同学最终未转账。



5. “仙人跳”类型诈骗

刘女士通过某交友平台结识了一名“网友”, 两人聊得很投机, 见面后发生关系并拍摄部分裸露照片。该“网友”之后向刘女士索要“封口费”, 否则威胁把这些照片公之于众。刘女士犹豫再三最终选择报警。

6. 以换汇名义实施的诈骗

杜同学在某留学生微信群中看到一则“留学生急换欧元支付学费”的消息, 便与当事人取得联系约定线下交易。在谈妥汇率后, 杜同学将2000欧元现金交给对方, 对方也通过微信转来了“银行转账凭证”截图, 并表示因周末关系钱款到账需迟滞数日。但一周后, 杜同学仍未收到汇款, 联系银行后才得知对方提供的是一张修图过的虚假转账凭证, 而对方早已将杜同学“拉黑”。

7. 以租房名义实施的诈骗

宋先生在某社交软件上看到了一则租房广告, 与“房东”联系后, 为稳妥起见, 宋先生要求与“房东”线下见面看房。看房后, 宋先生对房子非常满意, 现场与“房东”签订了合同, 并按“房东”要求用现金支付了相当于三个月房租的押金, “房东”也很“守信用”, 马上给了钥匙。次日, 宋先生拿着钥匙入住时, 发现钥匙、“房东”及合同都是假的, 该房是“房东”在网上订的民宿, 而“房东”已把宋先生拉黑。



8. 以转售演唱会门票名义实施的诈骗

查同学在社交平台上看到有人转售某热门演唱会门票, 即私信当事人溢价购买, 但在演唱会门口被工作人员阻拦, 系统显示该门票已被使用。由于门票为电子版且大都为非实名制, 可能出现一票售多人情况, 建议通过官方渠道购票和退票。

9. 以收购二手手机名义实施的诈骗

杨同学通过网络平台结识一名网友, 对方以收购二手手机为由, 诱导杨同学前往一偏僻地点进行交易, 并伙同其他同伴将杨同学劫持, 逼迫其前往附近自动取款机提取现金。操作间隙, 杨同学通过微信向同学张某发送了求救短信及实时定位。张某收到求助信息后随即报警, 并驱车前往现场。在多方共同努力下, 警方最终将杨同学成功解救。

10. 以刷单返利名义实施的诈骗

徐先生在某软件上刷到一个“招募网络开店合伙人”的短视频, 对方表示只要注册网店, 垫款“做任务” (点赞、领红包、关注公众号等) 即可获得丰厚提成。在“合伙人”演示下, 徐先生很快做成了几单“生意”, “合伙人”也按约定支付了佣金。徐先生觉得有利可图, 便在“合伙人”诱导下继续充值, 但此后在徐先生要求提取佣金时, 对方以“系统维护”“操作异常”“账户冻结”等由一再拖延, 最终导致徐先生血本无归。

应对建议:

- **不轻信:** 陌生链接不点, 陌生电话不信。
- **不泄露:** 不对外提供验证码、银行卡密码等信息。
- **不转账:** 凡是要求向陌生账号汇款的, 一律挂断。

求助渠道:

- 遭遇诈骗请立即向法国警方 (电话 17 或 112) 报案。
- 涉及国内银行卡、账号, 请及时拨打国内 110 或 96110 (反诈专线)。