你一定会遇到电信网络诈骗！

这不是危言耸听，更不是标题党，电信网络诈骗已经渗透到你生活的每个细节，让你防不胜防！

近年来，随着网络技术的飞速发展，电信网络诈骗等非接触网络犯罪在我国发展蔓延，犯罪手段多、变化快，给人民群众造成巨大经济损失。

经对一年来我市发生的电信网络诈骗案件分析发现，受骗事主的年龄从 9 岁儿童到 90 岁老人，各个年龄段均有；性别上男性、女性比例基本均衡；身份从教师、医生、会计、企事业单位领导，到企业员工、私营企业主、在校学生、无业人员，覆盖各个领域。犯罪手段既有冒充公检法等政府机关诈骗，冒充领导、老师诈骗，冒充购物客服诈骗，也有刷单诈骗，贷款诈骗，网络交友引诱投资、赌博诈骗，还有购买游戏装备、点卡诈骗，游戏带玩诈骗，裸聊敲诈，投资诈骗等等，种类繁多。

北京市反电信网络诈骗犯罪中心，北京市公安局刑事侦查总队根据当前犯罪手段特点，梳理了当前相对多发的十六类诈骗手段。通过真实案例，从易受骗群体、骗术揭秘、话术关键点等三个方面对案件进行剖析，并做出防范提示。

请您抽出宝贵时间，认真阅读本宣传册的案例，了解防范知识，提高防范意识，保护财产安全。

全民反诈，首都无诈！我们一起努力。

兼职刷单诈骗

真实案例

2020 年 9 月，事主王某在暂住地加入了一个微信群，群中有一名陌生人添加他为微信好友，并询问他是否想刷单兼职挣钱。王某同意后，对方通过微信发给王某一个二维码，要求其扫码支付 100 元。支付成功后，对方通过支付宝向王某返款 105 元。随后，王某又通过微信向对方支付了 8 次共计 7600 元，但是对方以王某支付有误、系统故障、订单任务未完成等理由拒绝返还佣金和本金，并要求其继续刷单转账。王某发觉被骗后报警。

骗术揭秘

第一步：发布网络兼职刷单信息，寻找被骗对象。骗子通过微信、QQ 等社交软件发布兼职刷单信息。吸引有兼职挣钱想法的人员与其进行沟通。

第二步：首笔刷单返现，建立信任。事主刚刚接单的时候一般都比较警觉，所以往往都是小额参与。骗子会在事主第一笔刷单之后，将本金和佣金及时进行返还，目的是与事主建立信任，为之后的大额诈骗进行铺垫。

第三步：大额刷单不返本金，诱使事主追加刷单资金。建立信任后，事主进行大额的资金投入。此时骗子有的会只返还佣金不返还本金，有的甚至本金、佣金都不返还。并以需要凑单、验证之后才能批量返还，诱使事主不断追加资金投入。直到事主自己醒悟，意识到被骗为止。

话术关键点

1. 在网购电商初期，确实有过网络刷单的情况，使事主认为刷单是真实存在的，但是目前该行为已被禁止。

2. 刷单的方式分多种。有的骗子会制作虚假网站，诱使事主直接进行转账；有的会让事主在真正的电商购物平台上购买点卡、充值卡等物品，之后骗取充值卡的电子信息；有的骗子直接微信要求事主扫码支付。

3. 在第一笔交易完成后，骗子会提出之前刷单金额太少，要想挣钱就要进行大额的交易。当事主进行大额支付后，骗子就会告知事主，由于系统或其他原因，无法单笔返还，需要多笔交易达到一定金额才能够返还资金。而当事主进行了几笔交易后，骗以还会以需要凑单、验证之后才能批量返还等理由，诱使事主不断追加资金投入。而事主往往抱有侥幸心理，继续投入资金。

易受骗群体

日常有空闲时间，想通过寻找兼职来赚取补贴。易发案年龄段为 18-35 岁青年群体较多。学生、在家待业、务工人员等经济基础较薄弱群体。

警方提示

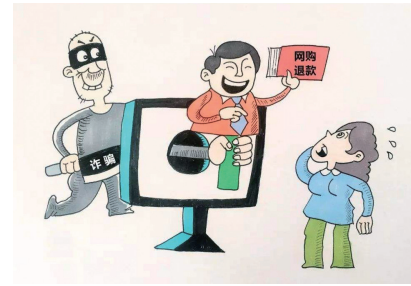
1. 刷单就是诈骗！坚决不能参与。
2. 刷单是违法行为！坚决不能参与。
3. 当收到兼职刷单的信息时，无论真假都不要参与。如果是真的，你将触犯法律，属于违法行为；如果是假的，那么你将面临资金损失。

刷单是什么？刷单一个电商衍生词。店家付款请人假扮顾客，用以假乱真的购物方式提高网店的排名和销量获取销量及好评吸引顾客。刷单一般是由卖家提供购买费用，帮指定的网店卖家购买商品提高销量和信用度，并填写虚假好评的行为。刷单是一种非法的商业模式和营销行为，也是一种虚假广告宣传和不正当竞争行为，侵害了消费者的知情权，违反了《广告法》、《反不正当竞争法》、《电子商务法》等法律法规。

目前，刷单被犯罪分子利用，实施诈骗。

冒充网购客服诈骗

真实案例



2020 年 9 月 5 日，事主王某（女，38 岁，某研究机构工作人员，硕士）接到一个自称是某网购电商平台客服的电话。对方说事主在该网上买的一款护发精油有质量问题，商家要收回，并两倍赔付。事主今年 6 月份确实在该电商平台买过同款产品，因此推断对方说的是此笔交易。对方在电话里让事主看自己的网购平台账户是否收到退款，并称赔款已经打到事主的网购平台账户了。在事主查询后称没有收到理赔时，对方说可能是电商一方操作有问题，并称系统授权理赔需要认证流水，走流程，让事主先在“借呗”上借钱到自己的银行账户，再把银行账户的钱转给对方，对方会再通过支付平台返还给事主。事主称不会操作，对方立即让事主添加其 QQ 好友，并打开 QQ 视频通话的屏幕分享功能，这样对方就可以看到事主的手机屏幕了。事主将自己在该平台的账号和密码告知对方后，对方登陆事主的账户，并给客服发送一个二维码。随后，客服向事主发送 2 个银行卡卡号，要求事主通过某平台的借款功能和多个银行的借款功能进行借款，并全部转入了上述两个账号。事主共计被骗 12 万余元。

骗术揭秘

第一步：非法获取信息。犯罪嫌疑人通过非法渠道获取群众网购的信息，然后以客服的名义联系。

第二步: 联系群众“退款”。谎称网店的这次交易出现了问题，以退换货、重新确认、补偿等为由，要求消费者重新执行指定的操作。有时还会以给予打折来吸引消费者。

第三步：实施诈骗。要求群众使用“借呗”等贷款平台贷款，将钱款打入骗子提供的账号，谎称钱在完成退款交易后会转入群众账户。

第四步：使用非正规渠道。骗子在诈骗时使用的是非官网渠道或第三方支付平台，而是要求直接打款或转账从而进行诈骗。

话术关键点

1. 犯罪分子自称是某网购电商平台客服，以事主网购的商品存在质量问题，商家要收回、理赔等理由博得事主信任。
2. 要求事主查看自己在网购平台的账户是否收到退款，并称赔款已经打到事主的网购平台账户了。
3. 谎称系统授权理赔需要认证流水，走流程。故意将流程说得繁琐，使事主产生让客服替自己解决问题的愿望。
4. 让事主添加对方 QQ 好友，并打开 QQ 视频通话的屏幕分享功能，这样就可以看到事主的手机屏幕。
5. 要求事主告诉对方自己的平台账号和密码，登陆事主的平台账户。

6. 发送二维码和银行卡号，要求事主在支付平台、银行的网上银行渠道打开借款功能，要求把钱（除赔偿之外）全部转入对方提供的账号。

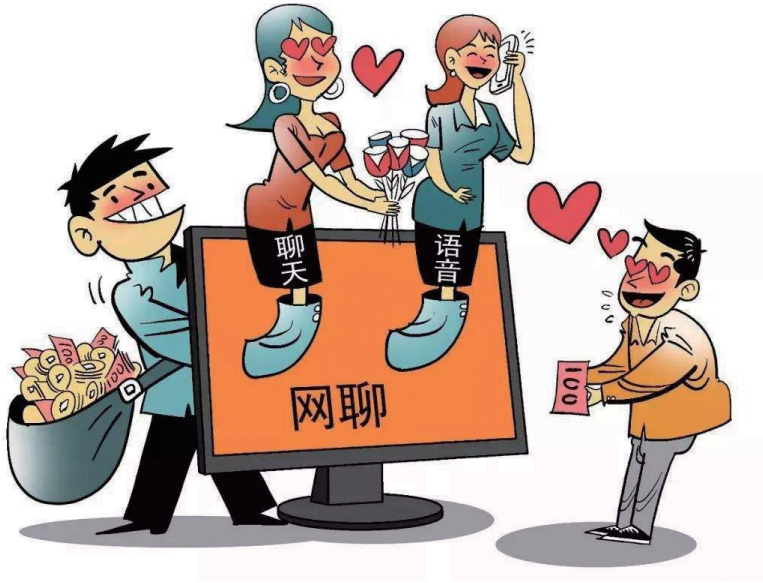
易受骗群体

骗子掌握事主的网购信息，迷惑性较大。20–35 岁青年网购群体较多，缺乏核验意识，不了解退换货规范流程或途径。

警方提示

1. 网购平台的客服不会涉及商家退赔的事情，更不会替商家向消费者进行赔款；客服不会让消费者查询赔款，也不会知道赔款是否已经到账；对方声称赔款未到账可能是电商一方操作有问题，实际上客服是不可能知道是什么问题的。
2. 系统理赔不是电话客服的工作。客服来电只能起到通知义务，不会涉及理赔及系统认证的操作问题，并且理赔是不能靠系统完成的，系统只能起到管理的作用，而不能真正的实现理赔。
3. 客服只会用一种沟通方式与消费者交流。电话客服只会在电话里与消费者对话；平台客服只会在该平台内与消费者交流，不会跨越两种沟通方式联系消费者。
4. 客服不会向消费者发送二维码。
5. 要通过官方公开的方式向电商平台核实退赔事宜。且要在挂断电话的情况的下，通过原购物平台查看自己该笔商品的处理情况以及是否收到理赔款。
6. 退款、退货要通过官方平台，通过原购物渠道办理，不要使用对方发送的链接、二维码等。

裸聊敲诈



真实案例

2020 年 8 月，郝某在家中搜索色情信息并添加了一个 QQ 号。后对方给其发了几张黄色图片，称可以一对一裸聊。郝某遂点击对方发来的链接，下载了一个直播 App，然后与一女子相互自慰。大约 3 分钟后突然黑屏。随后，对方通过 QQ 将其手机通讯录截屏和自慰视频发了过来；并称如果不想视频被转发给这些人就马上转账 3000 元。此后，对方又多次向郝某敲诈，共计 63000 元。郝某无力承受后报警。

骗术揭秘

第一步：获取公民信息，筛选对象。犯罪分子通过非法渠道获取医生、教师、公务员等机关、事业单位人员群体的姓名、单位、手机号码、微信号等个人信息。

第二步：添加好友，网聊铺垫。犯罪分子以带有美女头像的微信号或者在网上发布一些色情信息，寻找事主主动上钩，添加上述特定群体为好友。若受害者与其互加好友，然后发送黄色图片或者视频，吸引宅男一类人的兴趣。

第三步：视频聊天，录制“证据”。嫌疑人用事先录好的淫秽小视频吸引受害人，并以看表演，真人一对一来引诱受害人下载专属 APP。该 APP 由嫌疑人定制，伪装成视频直播软件，其实是获取受害人通讯录列表和开启摄像头权限的。然后发出视频聊天邀请引诱受害者裸聊。在此过程中通过不断言语刺激，让受害人暴露面部和下体，犯罪分子将受害者裸聊过程录制成视频作为后续敲诈的“证据”。

第四步：“花钱消灾”，反复敲诈。在收集到“证据”之后，对方会以散布裸聊视频或将视频向受害者单位举报或发给亲属朋友等对受害者实施威胁，并多次敲诈勒索。

话术关键点

1.QQ 添加好友后发送黄色图片和淫秽视频引诱受害人，之后以看表演、真人裸聊诱导受害人进一步操作。

2. 向受害人发送带有木马的二维码或链接，要求下载。

3. 当受害人按照发来的链接点击下载伪装成直播平台的APP 后，嫌疑人诱导受害人赶快下载开始裸聊。
4. 当受害人下载并授权麦克风、通讯录、摄像头之后，嫌疑人会催促受害者脱衣服、并且对着摄像头自慰以便拍摄。
5. 在获取受害人通讯录和自慰视频以后，根据受害人的身份特点，向受害人勒索钱财；并根据受害人的态度和情绪反应，反复勒索。

易受骗群体

受害者以男性为主，多为 25-35 岁单身男青年，在互联网主动搜索交友软件或平台。

警方提示

1. 不要随意点击陌生链接。
2. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。
3. 不能随意授权手机权限，通讯录、摄像头、麦克风权限要守住。
4. 不在网是对身份不明的人员裸露身体。
5. 不随意浏览不健康的网页。

冒充公检法诈骗

真实案例

2020 年 7 月，某大学教授李某接到自称是“通讯管理局”的电话，对方说李某名下的手机存在发送大量诈骗短信的情况，要对其手机卡进行强制性停机，李某并未办理对方所说的手机卡，但是因对方说出了其办卡的具体时间、地点，同时报出了其身份证号码以及家庭住址等信息，在李某否认后，对方说有可能是因为个人信息被他人冒用了。并说“通讯管理局”与“公安局”有合作机制，可以把电话直接转接到“上海市公安局”。电话转接到“公安局”后，接电话的“民警”不但确认李某名下的确有这手机号码，

而且他名下某张银行卡涉嫌帮助某犯罪团伙洗钱，对他的“通缉令”也正下发之中。如果想要洗脱罪名就必须配合“警方”工作接受调查，要求李某添加对方 QQ 好友，配合“警方”进行“远程笔录”。对方通过 QQ 给李某发送了“警官证”以及“通缉令”等法律文书。同时要求李某将手机设置呼叫转移，并新买一部手机和新卡单线联系；且对此事要绝对保密，不但对家人朋友保密，对当地警察也要保密，因为警察也有涉案，不能走漏消息。否则要承担“法律责任”。李某连续几天都在配合对方“调查”，告知对方自己的银行账户卡号等基本的信息以及密码。直到反诈中心发现此情况及时劝阻，李某这才恍然大悟。

骗术揭秘

第一步：建立信任，吸引被骗事主。在此环节中，骗子会冒充通信管理局、卫健委、疾控中心等国家单位与与事主进行沟通联系。告知一些涉及事主个人利益的受损的情况，而事主能明确了解。所谓的情况他而本人并没有参与。当事主进行辩解，对方就会很自然的告知事主，是由于身份信息被泄露才造成这样的结果。之后会帮事主转到公安机关进行解决。

第二步：树立权威，震慑事主。当所谓的“公安机关”与事主联系后。“民警”会先了解事主一些基本情况，然后会明确告知事主就是涉及案件的犯罪嫌疑人。用突如其来

的言语震慑住事主。

第三步：深度洗脑，控制住事主。骗子会不断变换身份，利用不同的道具、话术告知事主存在犯罪行为。让事主相信自己确实涉嫌案件，并且如果想洗罪名必须配合“公检法”机关的调查。

第四步：转账汇款，榨干事主的资金。在事主被控制住后，对方就会要求事主进行转账汇款，将资金转入“公安机关”的“安全账户”或者盗刷事主资金，有的甚至还会要求事主到贷款公司进行贷款或者抵押，之后再将这些资金转给骗子。

话术关键点

1. 骗子有不少是境外来电，“00”开头或者“+”开头的都是境外来电，谨慎接听。
2. 骗子无论一开始冒充哪个单位最后都会绕到身份信息被盗用需要联系公安机关解决。
3. 骗子为了能够成功实施诈骗，一定给事主制造一个心理或者物理上的密闭环境。避免因为他人的介入造成事主在骗局中清醒。例如：保密不能告知他人、手机开呼叫转移、购买新的手机号使用。到酒店、KTV 开房等。
4. 要让事主最终相信自己确实涉及案件，骗子会使用一些道具，例如电话中会让事主听见他们用电台进行对话。让事主看自己的通缉令等。
5. 要求事主将资金转入对方提供的，所谓的公安机关的“安全账户”内，进行资金核查。

易受骗群体

骗子掌握事主的部分个人信息包括姓名、证件号码等，可以叫出事主姓名，并核对证件号码。易发案年龄段为25-55岁群体较多，不分职业。

警方提示

1. 公安机关的电话不可能由任何部门进行转接，能把电话转接到公安机关的一定是骗子。
2. 公安机关不会通过电话、QQ、微信等社交软件在线制作笔录。在电话里办案，还让事主看自己通缉令的都是骗子。
3. 保护好自己的个人信息，特别是银行卡账户、密码、验证码等信息。不能随意告知他人，也不能在陌生网站上进行填写。
4. 公检法机关没有“安全账户”，凡是要求把钱转入“安全账户”的都是骗子
5. 陌生人发来的链接不要点击，避免手机中毒被远端控制。
6. 如果拿不定主意，要通过拨打110或者到属地派出所进行咨询。
7. 可以下载北京市公安局开发的“全民反诈”APP，通过“身份验真”模块，要求做笔录的“民警”进行身份验证。
8. 96110是反诈专用号码，如果有96110来电一定及时接听。
9. 部分公检法诈骗案件会要求事主安装XX公安局APP，需要通过链接下载xx.apk的安装包且官方应用市场无法查询到该APP。该类APP未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。

贷款诈骗（一）

真实案例

2020年9月1日，事主刁某向丰台分局长辛店派出所报警称，8月30日15时许，事主在家中用手机上网时，网页弹窗弹出了一个网络贷款的广告。事主点击后下载了一个叫“微粒贷”的APP。进入该APP后，事主按照要求填写了个人的全部信息（包括姓名、身份证号、手机号、住址等），并提出需要贷款30000元的请求。大约5分钟后，APP内的一个客服人员与事主文字聊天，详细询问了事主的贷款金额、贷款期限。在得知事主想贷款30000元，期限两年后，客服通过计算称每月要偿还1430元，两年期共还款34000元。事主同意后，对方称需要提交材料费、邮递费、密码提现工本费等共计1500元，并称贷款成功后一并退还给事主。事主就按照对方要求，将自己的银行卡号输入APP，后按照对方提供的农业银行个人账号汇款1500元。汇款成功后，客服称事主账号输入错误，账户已经被冻结，事主经核实发现确实错了一位数。对方让事主再支付12000元解冻费，贷款成功后也一并退回。事主汇款

后，客服又称事主输入账号时没有填写姓名，还需要再转12000元解冻费，这笔款也会退回。事主又按照要求汇款12000元后，客服再次称事主存在恶意贷款风险，需要交30000元回档押金。此时事主开始怀疑是否被骗，要求退款。但客服称此时不再申请就属于事主违约，即使退款，也要扣30%的违约金。事主称只能筹款2万元，客服称能帮忙垫付1万元完成手续。随后事主又汇入对方提供的账户20000元。20000元汇入后，客服改口称不能垫付了，需要事主再支付10000元，否则无法贷款。事主发现被骗遂报警，共计被骗人民币45500元。

骗术揭秘

第一步，发布广告，吸引贷款群众。通过手机广告弹窗，诱导有贷款需求的群众安装伪造贷款APP软件。

第二步，谎称严格审核，诱骗群众。要求群众在APP上填写详细的个人信息，回答问题，制造出手续繁琐、审核严格的假象，让群众误以为很正规，信以为真。

第三步，要求缴纳费用，实施诈骗。在群众信以为真后，谎称贷款额度已批准，以需要缴纳会员费、认证费、先期贷款利息等各种名义，诈骗事主钱款目。

话术关键点

1. 通过发布广告，谎称公司贷款便捷，放款速度快，费用低，吸引群众。

2. 向群众发送二维码链接，要求扫码申请贷款。

3.认真询问群众以往贷款、征信情况，制造正规公司的假像。

4. 第一步先让事主支付手续费等小量资金。当事主上当支付后，陆续加码，以威逼、利诱等各种手段，要求事主支付刷流水、解绑定等各种费用，增加诈骗金额。

易受骗群体

有贷款需求想要快速获取贷款额度，无法从正规渠道获取贷款，缺乏对对方身份核验意识。18-35岁青年群体，学生、务工人员等经济基础较薄弱群体。

警方提示

1. 贷款要通过银行或正规的贷款公司。
2. 贷款时要通过应用市场下载银行、正规贷款公司的APP或登录官方站，不能通过扫描二维码的方式下载APP。
3. 凡是在放款前索要费用的，都是诈骗，不能相信。
4. 安装“全民反诈”APP，了解反诈知识；从源头屏蔽涉诈软件，接收警方防范提示。
5. 需要通过链接下载xx.apk的安装包且官方应用市场无法查询到该APP。该类APP未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。

贷款诈骗（二）

真实案例

2020 年 8 月 31 日，群众李某向丰台分局新发地派出所报警称，8 月 30 日，一个自称“京东金融”业务员的微信号（微信昵称：J.D 业务员）请求添加事主为好友。事主通过后，对方自称是京东金融业务员，能办理贷款。事主目前确实资金紧张需要贷款，但又怀疑微信操作贷款的真实性。双方通过微信交流，事主表露了想贷款人民币 5 元万的意向。对方称是正规金融贷款公司，一切手续都在正规 APP 软件操作，并给事主发送了一个二维码名片。事主通过扫描二维码安装上一个“京东金条”的 APP，按对方要求在 APP 中填写个人资料。对方称需要严格审核，详细问询了事主有没有贷款逾期、信用不良记录的情况。随后，事主看到这个“正规”APP 上详细的调查，因此

对贷款公司深信不疑。8 月 31 日，对方微信通知事主贷款申请通过审核，需要注册一个中级会员才能贷款。中级会员注册费 899 元，如果贷款失败，这笔钱会自动退回。对方通过微信发给事主一个建设银行的个人银行账号，事主没有怀疑就转账 899 元。但 APP 客服答复，事主在软件内输入的信息错误，无法转账，需要提交贷款额的 30% 重新认证，共计 15000 元。事主此时想拒绝再次打款，并要回之前的 899 元。但微信客服称这样属于违约，会影响个人征信，并会移交司法部门处理；并称该 15000 元在贷款成功后会一并退回。事主只好再次通过对方提供的另一个建设银行个人账号汇款 15000 元人民币。汇款后，事主发现在 APP 内仍然无法提现贷款，而客服还要求偿还一期的利息，验证偿还能力。事主发觉被骗后报警。

骗术揭秘

第一步，发布贷款信息，联系群众。冒充贷款公司员工添加事主微信，也可能长期潜伏在事主微信群中，掌握事主具体情况，并在朋友圈发布贷款广告。通过微信朋友圈宣传、主动联系的手段，诱导事主申请贷款。

第二步，发送涉诈二维码，欺骗群众。伪造知名金融公司的 APP，向群众发送二维码，要求添加二维码并填写个人信息和贷款信息。

第三步，谎称严格审核，诱骗群众。要求群众在 APP 上填写信息、回答问题，制造出手续繁琐、审核严格的假象，让群众误以为很正规，信以为真。

第四步，要求缴纳费用，实施诈骗。在群众信以为真后，谎称贷款额度已批准，以需要缴纳会员费、认证费、先期贷款利息等各种名义，诈骗事主钱款目。

话术关键点

1. 自称正规贷款公司的业务员，要求添加好友。
2. 谎称公司贷款便捷，放款速度快，费用低，吸引群众。
3. 通过微信、QQ 等途径向有意向贷款的群众发送二维码或链接，要求扫码申请贷款。
4. 认真询问群众以往贷款、征信情况，制造正规公司的假像。
5. 第一步先让事主支付手续费等小量资金。当事主上当支付后，陆续加码，以威逼、利诱等各种手段，要求事主支付刷流水、解绑定等各种费用，增加诈骗金额。

易受骗群体

有贷款需求，想要快速获取贷款额度，无法从正规渠道获取贷款，缺乏对对方身份核验意识的人群。易受骗年龄段为 18–35 岁的青年。学生、务工人员等经济基础较薄弱群体。

警方提示

1. 办理贷款要通过银行或正规的贷款公司。
2. 贷款时要通过应用市场下载银行、正规贷款公司的 APP 或登录官方站，不能通过扫描二维码或点击链接的方式下载 APP。
3. 凡是在放款前索要费用的，都是诈骗，不能相信。
4. 安装“全民反诈”APP，了解反诈知识；从源头屏蔽涉诈软件，接收警方防范提示。
5. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到的 APP，都是未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。

冒充医院、学校领导等熟人添加微信、QQ 诈骗

真实案例

2020 年 9 月 18 日，位于我市东城区的一所全国著名医院的 3 名医生先后收到微信昵称为院长姓名的人发来的添加好友请求，而且微信头像也是院长本人的工作照。医生们通过医院相关部门进行核实，发现该微信号并非院长的号码后没有添加好友，未造成损失。

2020 年 9 月 15 日，我市一所高校的多名老师也反映，有人冒充校长微信添加老师为好友，并以给领导送礼的名义让老师们给指定账号转账 2 万元。该微信头像是网络上的校长照片。老师们没有转账，也没有造成损失。

骗术揭秘

第一步：非法获取信息。犯罪分子首先通过不法渠道获取了医院、学校等单位领导、员工的通讯信息，以及单位的组织架构。

第二步：添加好友。以单位领导的名义添加员工的微信好友，为增加可信度，会通过网络等渠道获取领导的照片，作为微信的头像。

第三步：实施诈骗。在员工添加了“领导”的微信后，“领导”一般会对员工嘘寒问暖，拉近感情。之后就会以给领导送礼、给亲友资助但本人不方便为由，要求员工先向指定的账户转账汇款，并称稍后会将钱款还给员工。甚至为了增

加可信度，会索要员工的银行卡号，制作虚假的转账凭证，证明已将钱款向员工转账，请员工向指定账户转账。

话术关键点

1. 利用网络上的领导照片作为微信头像，增加可信度。
2. 添加好友后，可能对员工嘘寒问暖，拉近感情，增加信任。
3. 犯罪分子会抓住员工对领导的敬畏、不敢质疑的心理，要求员工按其要求转账汇款。
4. 使用“尽快”“立即”等词语制造紧张气氛，让员工尽快转账汇款。

易受骗群体

单位员工，无领导联系方式或缺乏同领导沟通，若未经核实容易上当受骗。

警方提示

1. 遇到领导要求添加微信、QQ 等即时聊天工具时，可以通过单位人事部门、同事其他渠道进行核实。也可以使用“全民反诈”APP 的“身份验真”功能，要求对方进行实名身份认证。
2. 如果已添加好友，可以利用单位内部的一些情况，从侧面了解核实对方身份。
3. 如果对方要求转账、汇款等，务必通过电话、见面等方式核实对方身份，不要轻易进行转账汇款。
4. 注意保护个人信息和单位信息，防止犯罪分子利用这些信息精准实施诈骗。

冒充快递实施诈骗

真实案例

2020 年 9 月 1 日 13 时 30 分许，事主胡女士（北京某协会秘书长）在家中接到一个陌生电话。对方称事主的一个快递丢件了，稍后会有人联系事主办理理赔。几分钟后，事主接到另一个电话，称给事主办理理赔，并让事主添加对方 QQ 好友。事主添加对方为 QQ 好友后，对方发来了一个二维码，让事主用某支付软件扫描这个二维码，然后在弹出的界面上填写事主姓名等个人信息及银行卡信

息。紧接着，事主的手机收到了好几条验证码短信，对方在电话里要求事主告知验证码。事主由于要开会，在没有细看短信内容的情况下就把一条验证码告诉了对方。随后，事主意识到可能被骗，没再继续告诉对方其他验证码，并将支付软件绑定的 2 张银行卡冻结。经事主查询交易流水，发现其中一张银行卡上损失人民币 9980 元。

骗术揭秘

第一步：冒充快递公司给事主打电话称快递丢失，可以办理理赔。

第二步：冒充快递公司理赔人员，添加事主微信、QQ 好友，发送带有木马病毒的二维码，要求事主扫码并填写个人信息。

第三步：索要事主验证码实施诈骗。

话术关键点

1. 第一个嫌疑人打电话告知事主有快件丢失，稍后有人为受害人办理理赔，这是第一步的铺垫，让受害人在心理上有一个关于理赔的预设。

2. 第二个嫌疑人拨打事主电话，自称是帮助事主理赔的工作人员。因受害人事先心里有过预设，因此会同意对方因理赔事宜而对提出的要求。

3. 对方要求添加 QQ 或者微信好友，通过发送二维码的方

式向受害人手机植入病毒或者诱导事主进入对方后台服务器，填写银行卡信息。

4. 当事主手机收到验证码后，催促事主告知验证码，以刷卡消费或将事主卡内的钱转走。

易受骗群体

缺乏核验意识，不了解退换货规范流程或途径的群体。易发案年龄段为 20-35 岁的青年网购群体。

警方提示

1. 接到快递丢失可以办理理赔的电话，要通过原购物渠道了解具体情况，不要轻信一面之词，在心里预设快递丢失。

2. 不要轻易该添加陌生人为好友。正规客服更不会以此种方式和消费者进行沟通。

3. 不要随意扫码对方发来的二维码或点击链接，这很有可能是病毒或者恶意链接。

4. 不能将验证码告诉任何人。正规客服也不会向消费者索要验证码。

杀猪盘诈骗一（网络交友引诱投资理财）

真实案例

年轻的刘女士 (23 岁，医院护士) 单身独居。虽然高学历高收入，但婚姻大事始终没有解决。2020 年 8 月，偶然在家中刷微博时，看到一个叫“北京牵线月老”的微博群中有一男子发布了单身信息。刘女士与对方在微博群中简单沟通，随后对方主动要求添加刘女士 QQ。刘女士通过 QQ 空间了解到，对方是个阳光多金的帅气男性，自称是某企业高管，收入丰厚。两个人经过几天的聊天接触互生好感，每天都在 QQ 中甜言蜜语，对方表示要刘女士做自己女友，并主动向刘女士推荐投资黄金，希望一起挣钱共渡余生。刘女士根据对方提供的二维码扫码进入一网站，按照对方要求下载注册了“领峰国际”APP。后该男子指示刘女士购买黄金，称有周年活动这时充值可以有高于市面 30% 的回报。刘女

士于是尝试充值了 100 元。100 元投进去没多久后就有了 200 多元的收益。第二日，对方称有朋友是此款软件的工程师，发现了软件的漏洞，可以利用这些漏洞进行投资，获得可观的收益。对方让刘女士和自己一同继续购买比特币，刘女士在充值 1 万元购买比特币后，挣了 3000 元并成功提现。又过了几天，对方告诉刘女士，目前趋势比较好，希望增加投入，可以二次晋级成为黄金会员并将获得更高的收入。刘女士为了爱情和利益，一次性投入人民币 5 万元购买了比特币。当她想提现时却发现软件账户已无法登陆。联系对方称，由于之前会员活动充值人员过多导致系统瘫痪，需要暂时冻结账号，所以不能提现。如果想要解冻之前的账号需要向自己的账户充值 20 万元。刘女士随后给对方发送借钱解冻的信息，发现对方已将刘女士在 QQ 上拉黑。刘女士发现被骗后报警，实际损失人民币 47000 元。

骗术揭秘

第一步：发布交友信息，结交异性朋友。骗子通常会在各大单身交友群、交友软件、交友网站上发布信息，伪装自己高富帅或白富美的形象，在与你取得初步信任之后，对方会要求添加 QQ 或微信进一步了解，频繁与你聊天，让你对其产生信任，有些骗子甚至会对你关怀备至，迅速与你确定恋爱关系，让你对他（她）加深信任。

第二步：确定恋爱关系，推荐投资平台。到关系稳定之后，

骗子便开始怂恿你在他（她）们自制的网站平台购买投资理财等项目，大多数人都会试着小额投入几笔，骗子会通过后台操作，让你小赚几笔。

第三步：给予小额利益，诱骗加大投入。当你小赚尝到甜头之后，骗子会并声称自己已经掌握了这个投资软件的规律，或者了解这个软件的漏洞，只要跟着他（她）投资稳赚不赔。这时，你已经深信不疑，便往平台里面大量投入。

第四步：诈骗事主钱财，拉黑杀猪跑路。当事主投入大量资金之后，却不能提现。与对方交涉时，对方会让你继续加大资金投入，进行“解冻结”、“升级会员”。如果拒绝再投资就会发现之前的联系方式均被拉黑，对方已经消失得无影无踪。这时事主才发现被骗。

话术关键点

1. 通过网络结交异交异性朋友。如果网友是女性，则把自己包装成高富帅；如果网友是男性，则骗子包装成白富美。在最初的几日，通过甜言蜜语使双方感情迅速升温。
2. 自己是（或认识）投资平台的管理人员（技术人员），了解系统漏洞，但本人不能在公司投资。因此请男（女）朋友投资赚钱，然后二人可以实现经济自由，共同开启新生活。
3. 先投入小额资金进行尝试，等赚到钱要求不断加大投入。
4. 通过操纵后台肯定能让事主赚到小钱，并可以顺利提现。随后要求事主放心，加大投入。

5. 事主加大投入后发现不能提现。告诉事主平台正在维护或出现问题，总之是要事主再继续投资才能提现。

6. 当事主不想继续投入，只要求提现时，就会发现对方拉黑了之前的联系方式，消失了。

易受骗群体

在互联网主动搜索交友软件或平台寻找交友对象。25-55岁，单身群体较多。

警方提示

1. 提高防骗意识，保持良好的社交心态，在没有确定对方真实身份之前，警惕经济上的来往，不要向陌生人转账。也可以使用“全民反诈”APP 的“身份验真”功能，要求对方进行实名身份认证。

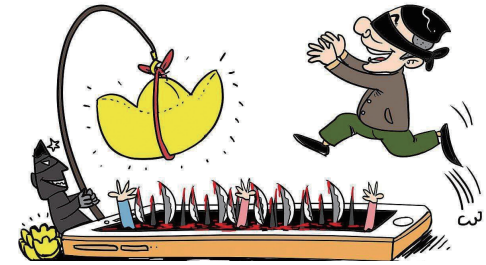
2. 保持正确的投资、理财观念，警惕不切实际的高风险投资。尤其是在网络交友中，若对方提到“博彩软件”“投资平台”等关键词，更要提高警觉。

3. 受骗后不要盲目相信网络上自称可以帮助追回或者拦截钱款的人，要第一时间拨打 110 或者去派出所，向公安机关进行报案，否则可能会遭遇二次诈骗。

4. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。

杀猪盘诈骗二（网络交友诱导赌博）

真实案例



2020 年 8 月， 赵女士（31 岁，研究生，医生）与男友分手后，通过“一周 CP”公众号，认识了一男性。对方自称 32 岁， 身 高 184，体重 74kg, 目前和朋友一起创业做数据维护 。短暂的聊天之后，赵女士与该男性一拍即合。男性表示赵女士就是自己一直寻找的灵魂伴侣，聊天过程中总是宠溺的称呼赵女士为小可爱。被家里催婚多年的赵女士，很快就陷入了这场“甜甜的恋爱”。一天，这个男性让赵女士用他自己的账号，在一个网赌平台上帮忙测试数据包。赵女身边有朋友是做软件开发相关工作的，经常需要测试各类平台，所以根本没有多想，就帮助对方用他自己的账号做了几期。一开始就说是数据测试，后面对方慢慢告诉赵女士这个平台可以挣钱，他已经靠这个挣了近 200 万。随着两人感情加深，对方建议赵女士也开通个账号和自己一起赚钱。起初，赵女士婉拒了对方。此后的一天，对方称要送赵女士一个礼物，礼物就是也在该博彩平台帮赵女士开了一个号，并充值了 3 万元，通过对方的操作该账户后续赚到了 5 万元。赵女士非常感动，紧接

着对方要求赵女士继续充值。赵女士想要先提现看看，没有充值。在提现过程中，系统提示其银行卡账户错误，赵女士联系在线客服，对方以账户被冻结为由，要求赵女士向账户内转账 6 万元人民币才能恢复账号。赵女士于是通过银行转账的方式向客服提供的行账户分 6 次转入人民币 5.5 万元后，系统提示需要继续充值 30 万人民币才可提现，此时赵女士意识到自己被骗遂报警。

骗术揭秘

第一步：包装自己吸引异性。网络交友类诈骗中，骗子通常会把自己包装成优质男女，依托各类网络社交平台（如：陌陌、探探、soul、抖音、keep、领英、微博等等），以完美的人设吸引异性，在获取对方信任后引其入套。

第二步：快速建立恋爱关系。骗子通常会在了解你很少信息的情况下，就表示自己已经奋不顾身的爱上了你，并想方设法在短时间内与你确认恋人关系。然后不断的认同肯定你，不断的和你说甜言蜜语，试图让你陷入爱情的陷阱。

第三步：想方设法推荐平台。骗子通常在与你确认恋爱关系后，以信任你之名，让你帮忙其查看余额或做测试等方式，向你透露出自己在投资理财平台或博彩类平台中的巨额收入，让你觉得有利可图，引导诱惑你一同进行投资。

第四步：获取信任引诱投资。骗子一旦取得你的信任，就会想方设法拉你入伙，让你充值。碰到警惕性高的事主，

骗子还会先给你充钱，以此取得你的信任，以达到骗取你钱财的目的。

第五步：小利诱惑大额杀猪。骗子在你小额投资后，会通过操纵后台让你获得赢利，并可以提现，诱骗你加大投入。一旦你投入大额资金，骗子就会骗钱跑路，一去不回。

话术关键点

1. 迅速建立恋爱关系。骗子会通过花言巧语让你以为开启了一场浪漫恋爱。“小可爱，吃饭了吗，要吃饭哦，饿坏了我会心疼的，你吃的什么呀，给我拍照看看呀，我也想坐在你对面吃饭”；“小可爱，我刚开完会，你再干嘛呢？工作太累就辞职吧，我养你啊”；“小可爱，你什么时候答应做我老婆呀，我不想太晚结婚，我想早点跟你一起生活”等等。
2. 告诉你一起赌博可以赚到快钱，然后在一起快乐生活。
3. 谎称帮助平台测试，让你见到赢利。或是自称是平台管理人员或技术人员，掌握系统漏洞，可以带你一起挣钱。让你投入小额资金进行尝试，如果能赚钱再加大投入。
4. 发送二维码或链接，让你下载所谓的平台或 APP。
5. 不断劝说加大投入。甚至通过操纵后台，给你账户充值，让你误以为对方有诚意，而且稳赚不赔。
6. 当你投入大额资金后就不能提现，再以平台账户被封为由要求继续加大投入才能解决。直到你发现异常或没有资

金投入，表示不再投入后，对方就拉黑之前联系方式逃跑。

易受骗群体

受害者多单身，25 – 55 岁较多，在互联网主动搜索交友软件或平台寻找交友对象。

警方提示

1. 谨慎添加陌生好友。网络世界虚虚实实、真真假假，网络交友一定要有戒心，不要过度透漏自己信息，以免给对方留有可乘之机，落入对方圈套。可以使用“全民反诈”APP 的“身份验真”功能，要求对方进行实名身份认证。

2. 切勿进行钱款操作。广大群众要为自己设一道安全阀，即在网聊交友中一旦触及投资、购物、借钱、转账等关键词就要立即进行自我警示（对方是否是骗子），在没有真正确定对方身份及用意时，切勿进行钱款操作。

3. 赌博、网络赌博都是违法行为，坚决不能参与。

4. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。

校园贷诈骗

真实案例

2020 年 9 月，张某报案称，9 月的一天，在家中接到陌生电话，对方称为响应国家号召让事主注销其校园贷账户，并让事主加其 QQ 联系，后事主张某按照对方要求通过二维码下载贷款 APP，将 APP 中额度取出后转给对方。后怀疑被骗报案。

骗术揭秘

第一步：拨打电话，以注销校园贷账号要挟。犯罪分子先通过电话，以注销校园贷，否则将会影响个人征信等问题为由要挟事主配合其操作。

第二步：添加 QQ，下载贷款 APP。要求事主添加其 QQ 号，指导事主根据其提供的二维码或链接下载安装贷款 APP 并提取额度，称此次操作为验证身份必要流程，否则将无法注销。

第三步：要求转账至回款账户，并称此次提取额度无需偿还。骗子提供“回款”账号，并称该账号为公司验证账号，此次借款无需偿还，目的是为验证身份注销校园贷。

话术关键点

1. 以注销大学期间注册贷款账户，否则将会影响个人征信等问题要挟事主配合。

2. 添加 QQ，以截图的方式指导事主下载贷款 APP 提取额度，验证身份。
3. 冒充正规贷款公司客服，指导事主通过二维码或链接下载注册 APP。
4. 口头承诺将提取的额度转账至回款账号后即可，APP 中额度无需偿还。
5. 全程未涉及事主个人存款等资金，全部为贷款 APP 中额度，因此容易迷惑事主。

易受骗群体

高校在校学生或毕业生。

警方提示

1. 可以通过拨打贷款公司的官方客服电话核实对方身份，切勿轻信陌生电话并配合其操作。
2. 切勿相信对方口头承诺，APP 中所贷款项无需偿还等承诺。
3. 任何以注销校园贷为由的电话都是诈骗电话。
4. 可以下载“全民反诈”APP，通过“身份验真”模块功能核实对方身份。
5. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。同时该 APP 后台数据缺乏监管，缺乏必要的安全保证。

网络游戏产品虚假交易诈骗

真实案例

2020 年 8 月，事主贾某玩手游全民突击时看到游戏大厅内有收购游戏账号的信息，事主添加对方 QQ，对方称要从网站赶集 561 平台交易。事主进入该网址，注册账号后，将自己的游戏账号挂上 1500 元卖。后对方通过 QQ 告知事主已购买可以提现了，事主提现发现被网站账户冻结，客服提示称账户输错需要充值 1500.1 元解冻，事主将 1500.1 元转账到客服指定银行账号。依然不能提现，客服又要求事主继续转账 6000.1 元。事主继续分两笔转账共 6000.2 元到指定账户，后客服和对方 QQ 均失联。事主意识到被骗后报案。

骗术揭秘

第一步：游戏内寻找目标，添加 QQ。在游戏的聊天中寻找有出售游戏装备或账号的事主，并添加对方 QQ，确认

交易流程。

第二步：QQ 指导事主在虚假游戏交易平台进行注册。QQ 指导事主在指定的交易平台进行注册。

第三步：提现失败为由，要求事主继续充值。以账号提现失败被冻结，解冻需要需要充值。后又以提现未预留 1 元被冻结，要求继续充值。

话术关键点

1. 在游戏中寻找有交易游戏账号需求的玩家进行QQ联系。
2. 虚假游戏交易平台，以账号被冻结无法取消为由要求继续在平台进行充值解冻账号。

易受骗群体

受害者多为游戏玩家，18–35 岁青年群体较多，缺乏游戏账号或装备交易经验，不清楚正规交易平台。

警 方 提 示

1. 认准官方游戏账号交易平台。避免私下交易。
2. 以账户被冻结，无法提现，需要继续充值才可以解封账号的都是诈骗。切勿按照对方要求继续充值，避免更多的经济损失。

冒充老板骗财务人员诈骗

真实案例

2020 年 5 月，某公司财务人员张某，在公司接到自称是北京某科技有限公司财务人员的电话，称有一笔 30 万元的汇款给事主公司，并确认了公司的账号，之后事主张某向公司老总余总核实了情况，余总答复说应该是管理费。而后事主添加了对方公司财务的 QQ 号（昵称财务小李），当天事主就被拽进一个 QQ 群，群里有“财务小李”和“余总”，“余总”通过 QQ 跟事主说由她来跟进此事。次日早上 9 时许事主通过 QQ 问“财务小李”汇款情况，对方回复马上汇款，上午 10 时许“余总”突然 QQ 联系事主说要给某传媒有限公司一笔 200 万汇款急需转账，让事主查询公司账有多少余额，事主查后显示 90 余万元。由于“余总”催的比较急，事主就没再当面与余总核实，就从余总的另一家公司调来 110 万元，共 200 万元分 6 次转账给“余总”提供的公司，之后经核实发现被骗立即报警。

骗术揭秘

第一步：骗取公司联系方式以及人员关系。骗子通过网络，查询到一些公司的人员通讯录以及公司人员层级关系。

第二步：山寨公司老板身份，加公司财务人员好友。在获取基本信息后，以公司老板的头像、名字注册微信或者QQ，加财务人员好友。

第三步：以着急汇款为理由，要求财务进行转账汇款。在成为好友之后，“老板”会与财务正常交谈，甚至会建立微信（QQ）群，几个人共同联系工作，实际上群里除了财务人员以外，都是骗子假扮的。在聊得差不多的时候，会以正在和某公司洽谈业务，需要转保证金、定金、货款等理由，要求财务及时进行转账。

话术关键点

1. 公司员工接到陌生电话或者邮件索要公司通信录以及询问老板和财务人员基本情况的，极有可能是骗子在提前获取信息，一定不能泄露。

2. 诈骗分子通过非法渠道获取企业及财务人员的信息，假冒企业老板的微信、QQ 等，添加企业财务人员为好友，再将财务人员拉入某公司的工作群，并在群内谈论某项工作业务。

3. 模仿老板的口吻向财务人员下达转账指令，并且该转账需要加急办理，手续后补。作案过程中诈骗分子充分

利用部分员工敬畏上司，不敢冒昧跟领导核实信息的可乘之机，让财务人员信以为真，将钱款打入诈骗分子指定的账户。

易受骗群体

发案群体为公司会计，缺乏核验意识，公司内部转账审核流程存在漏洞。

警方提示

1. 突然接到领导的微信、QQ 的新发好友申请，一定要进行电话或者当面确认核实。

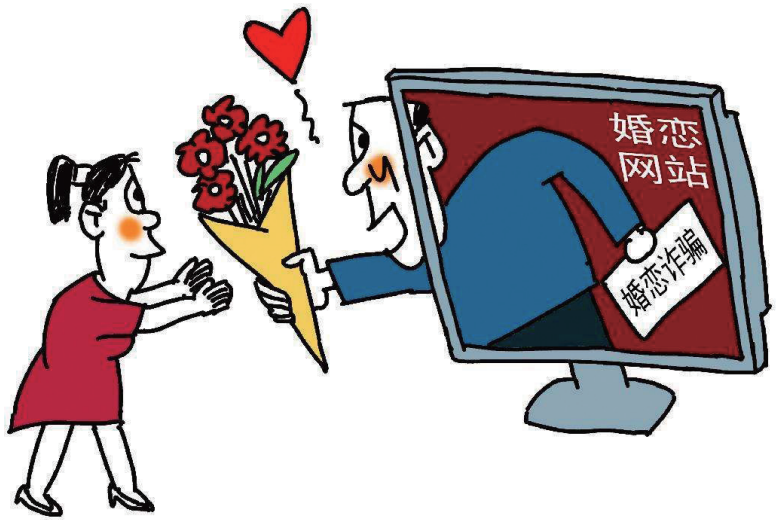
2. 涉及到公司转账情况必须与领导当面核实，走公司正规程序，履行相应的手续，确保万无一失。同事企业要制定严格的财务制度，杜绝快速办理绿色通道等情况，避免不必要的经济损失。

3. 核实对方身份可以通过“全民反诈”APP 中的“身份验真”模块，来核实对方身份，保证对方的真实性。

网络交友诈骗

真实案例

2020 年 2 月，事主郑某用手机上网时，一个陌生外国人主动与其聊天。对方自称是美国人，联合国驻叙利亚执行维和任务的少将武官。之后双方加微信聊天，并确立恋爱关系。2020 年 3 月，对方称将从叙利亚来中国与其结婚，但没有钱购买机票。理由是因未退役，钱都在联合国扣着不能用，退役后会一次性发放 300 万美金。事主郑某随后通过支付宝向对方转账 13500 元人民币。此后，对方又称因疫情防控，外国人到中国需要自费隔离，需要交纳 20000 元人民币和 20530 元人民币。事主郑某又通过支付宝分两笔向对方转账 20000 元和 20530 元。2020 年 4 月，对方称已经拿到退役款，在邮寄给事主的途中被



印度扣押，需要给印度方面交 17000 元人民币的税。事主郑某再次通过手机银行转账到对方提供给银行账号。之后，对方再次以物品被中国海关扣押为由，向事主郑某索要 79000 元人民币。事主郑某发觉被骗后报警，共计损失 71030 元人民币。

骗术揭秘

第一步：包装网络形象，自身定位外籍，维和官员、军官等成功人士。骗子在婚恋网站、社交网站上虚构个人信息，把自己包装成外籍，事业有成，多金富有的形象。

第二步：物色被骗对象，建立初步信任。通过虚构的成功人士形象，在网上寻找潜在的被骗对象。并在联系的时候骗取对方信任，迅速建立恋爱关系。

第三步：建立感情，用感情战胜理性。当事主完全坠入“爱河”之后，骗子就会利用到中国与事主结婚为由，以给事主邮寄礼物、个人物品，继承财产等各种理由要求事主“垫付”资金。而事主往往沉浸在“爱情”中不能自拔，按照对方的要求进行转账汇款。

话术关键点

1. 此类骗术中，骗子多在婚恋网站上物色目标，目标多为中年女性，特别时曾经受到过感情伤害的人是骗子重点关注的对象。

2. 骗子在包装自己的时候会用虚假的身份或者直接盗用他

人的信息。身份包装的越是显得高大上，之后就会越容易获得信任。特别是有部分骗子将身份包装成外籍，参加维和的官员或军人，以博取事主的好感并保持个人的神秘感。

3. 在骗取事主转账的时候，一般都会是将要到中国与事主结婚，所以邮寄礼物、邮寄个人物品，需要交纳关税等为理由。让事主以为既获得了“感情”又可以获得物质利益。

易受骗群体

受害者多单身，25–55 岁较多，在互联网主动搜索交友软件或平台寻找交友对象。

警方提示

1. 网络是虚拟环境，交友的前提是真实。所以在网络交友的时候一定要提前核实对方身份，并与身边亲友多沟通，以防落入对方陷阱。
2. 切莫被“感情”冲昏头脑，更不能抱着“虚荣心”的去交友。如果涉及钱财问题，不轻信对方任何说辞、借口，及时说不。
3. 核实对方身份可以通过“全民反诈”APP 中的“身份验真”模块，来核实对方身份，保证交友的真实性。
4. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。同时该 APP 后台数据缺乏监管，缺乏必要的安全保证。

网络赌博诈骗

真实案例

2020 年 4 月，田某报案称，自 2019 年 11 月其在家中添加一 QQ 好友，该人称可以带也一起赚零花钱。随后，对方给了其一个“亚游国际”的网站，并教会其在网站上投注。田某共计转账 109 万元。

骗术揭秘

第一步：添加好友，介绍赚钱之道。犯罪分子先通过 QQ、微信添加事主为好友，并告知可以带事主一起赚钱。

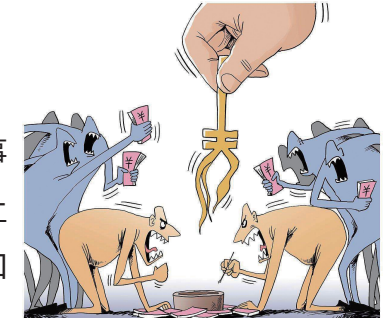
第二步：推荐网站，教授方法。向事主推荐赌博网站，并向事主教授操作方法。

第三步：发送诱饵，吸引投资。犯罪分子通过后台操作，让事主先赚到一部分资金，诱导事主后期不断加大投入。

第四步：后台操纵，不法获利。犯罪分子通过操纵后台，牟取利益。

话术关键点

1. 介绍赚钱之道，推荐网站。
2. 向事主教授操作方法。待事主学会后，通过后台操作，让事主先赚到钱，然后诱导其加大投入。



3. 此类案件不同于杀猪盘，没有了恋爱的过程，都是直接投注。
4. 利用网站或 APP，通过直播方式把线下赌场搬上网络。
5. 基于体育竞技、福利彩票的结果等进行外围赌博，比如赌球网站等。
6. 不法分子恶意利用移动支付平台和网络红包衍生出的新型赌博形式。
7. 不法分子利用一些休闲游戏平台，通过盗号、外挂等非法手段获取大量游戏币，再设立赌博骗局吸引玩家以牟利。

易受骗群体

有一定经济基础在投资或赌博平台进行下注的群体，25–55 岁群体较多。

警方提示

1. 施以小利。虽然大家都知道“十赌九输”，可很多人偏偏就觉得自己是“天选之子”。犯罪团伙就是利用这种心态，先让你赢一部分，再让人一步一步慢慢地堕入陷阱。
2. 有去无回。参赌者一开始要通过网银将赌资转入指定的账号，有时候用手机刷二维码，将钱转到赌博网站里。实际上，无论你是输是赢，由于犯罪团伙设了局，赌徒充值的钱只要进了他们的账户，最终就是肉包子打狗——有去无回。

3. 无法提现。有的人在某某网站侥幸赢了钱以后，申请提现时就会遇到“网站正在维护”的提示，让你明天再试。这些人暂时提不出钱来，就会忍不住继续去赌，然后把前面赢的和自己的本金全部输干净。即使没有输光，第二天再去提现时，还是说系统维护。如果去找客服，他们就会以各种理由和你拖时间，甚至是直接把你的账号禁封。
4. 虚假人气。通常新手登录平台后会发现，有很多人在里面玩，这种氛围使他们在心理上陷入集体无意识，觉得法不责众而产生虚假安全感，无法冷静思考。其实那些在玩的“人”，多数都是“机器人”。
5. 后台控制。网络赌博大坑中最可怕的，当然还是后台控制了。一般情况下，后台可以设置庄闲盈利点，可以在小的可控范围内让你赢钱，然后大多数情况下让你输。也有很多人在玩的关键时刻会遇到“网络不佳”。其实那并不是真的网络不佳，而是正在进行后台控制，让原本的赢局变成输局。
6. 抽水返点。大部分赌局的抽水返点是百分之几，玩家和庄家不停地赌，他们之间的胜率也会趋向平等。但庄家每一局都在“抽水”，即使玩家最终和庄家打成平手，因为抽水的机制，玩家的本金也会被庄家拿走大半。所以这就是为什么十赌九输，赢的只能是庄家。
7. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。同时该 APP 后台数据缺乏监管，缺乏必要的安全保证。

网络游戏陪玩诈骗

真实案例

2020 年 4 月，游戏高手王小姐正在玩一个爆款游戏。突然，有个陌生人发来信息，对方称有一个新款游戏，邀请王小姐这样的游戏高端玩家一起玩。随后，对方给王小姐发来一个二维码。王小姐通过二维码下载了这个游戏。此时，对方称需要充值才能开始，而且承诺自己充值会和王小姐相同，这叫做“共同成长”。此后没王小姐分几次充值了 3 万元，系统显示对方也冲了同等的数额。但是对方并不在游戏里发言，只是一直要求王小姐充值，后发觉被骗。

骗术揭秘

第一步：正规爆款游戏中寻找游戏高手。寻找目标，游戏高手一般具有一定的充值能力，因此骗子会主动寻找爆款游戏中的游戏高手邀请其下载这个新游戏体验试玩。

第二步：以等额陪同充值为由要求事主充值。以“共同成长”为由，承诺充值相同的数额，获取事主信任。

第三步：多次要求充值。骗子在游戏中不发言，只是一味的要求充值，当事主充入较大金额后，骗子就会拉黑消失。

话术关键点

1. 在爆款游戏中寻找具有一定充值能力的游戏玩家。
2. 以新款游戏为由，为其提供下载链接，并要求充值。
3. 以“共同成长”，承诺充值相同数额，获取信任。

易受骗群体

受害者多为游戏玩家，18–35 岁青年群体较多，具有一定的游戏充值能力。

警方提示

1. 不要从非正规渠道下载游戏，不要接受陌生人邀请玩其他不知名游戏。
2. 进行买卖等交易、充值时一定要选择正规第三方平台，谨慎交易；不要将自己的个人信息告诉他人。
3. 需要通过链接下载 xx.apk 的安装包且官方应用市场无法查询到该 APP。该类 APP 未经过应用市场审核，更容易造成手机信息泄露及银行卡被盗刷等资金安全风险。同时该 APP 后台数据缺乏监管，缺乏必要的安全保证。

断卡行动

真实案例

非法贩卖手机卡2020年2月23日，我市发生一起电信网络诈骗案件。犯罪分子使用一个北京号码（13*****1264）对事主实施诈骗。经工作查明，此涉案号码为嫌疑人江某于2月16日在一运营商营业厅办理，该人同时还开办多张手机卡，之后以每张40元价格卖给带队开卡人宋某。宋某随后将收购的手机卡转卖给电信诈骗犯罪团伙。电信网络诈骗犯罪团伙使用这些电话卡作为犯罪工具，对群众实施诈骗犯罪。

2020年4月14日，北京市公安局开展开打击治理“两卡”专项行动，将开卡人江某，收卡人宋某抓获。目前，收卡人宋某因帮助信息网络犯罪活动罪被逮捕，开卡人江某被刑事拘留并列入黑名单。2015年11月1日起实施的《刑法修正案（九）》增设了“帮助信息网络犯罪活动罪”，对明知他人利用信息网络实施犯罪而提供互联网接入等技术支持或提供支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

出租、出售手机卡、银行卡，支付账户、通讯账户，涉嫌帮助信息网络犯罪活动罪！

2015年11月1日起实施的《刑法修正案（九）》增设了“帮助信息网络犯罪活动罪”，对明知他人利用信息网络实施犯罪而提供互联网接入等技术支持或提供支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

2019年10月25日，最高人民法院、最高人民检察院公布了《关于办理非法利用信息网络，帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，自2019年11月1日起施行，对明知他人利用信息网络实施犯罪，为其犯罪提供帮助，“情节严重”的情形进行了明确，触犯法律的，将以帮助信息网络犯罪活动罪追究行为人的刑事责任。

警方提示

请保护好自己的身份证、手机号、银行卡（账户），严格落实实名制登记、使用。不要将自己的身份证、手机号、银行卡（账户）、支付账户、即时通讯账户等转借、转租、出售给他人，贪图这些小利可能影响个人征信，严重的将追究法律责任。

“全民反诈”APP

“全民反诈”APP 是由北京市公安局开发，用于打击防范电信网络诈骗犯罪的专用 APP。

该 APP 旨在宣传防范电信网络诈骗犯罪知识，提高群众防范电信网络诈骗犯罪的意识和能力，方便群众举报电信网络诈骗犯罪行为，提供电信网络诈骗案件线索，减少电信网络诈骗案件发生，避免群众财产损失。该 APP 设置了反诈宣传、预警提示、线索提供、指尖举报、风险提示、在线答题、安全检测等功能模块。群众可以通过“全民反诈”APP 了解最新诈骗手段伎俩、身边发案情况。

“96110”反诈骗专用号码

96110 是我市反电信网络诈骗犯罪专用号码，用于对群众进行预警劝阻，案件回访，防范提示及反诈宣传。如有 96110 来电，您或您的亲友可能正在遭遇电信网络诈骗，请您及时接听，耐心回答提问。如果发现电信网络诈骗犯罪线索，您可以拨打 96110 电话或发送短信，也可以通过注册“全民反诈”APP，关注“北京反诈”微信公众号进行举报。您的举报，可以避免更多的群众遭遇电信网络诈骗犯罪。