经常有受害人问：“我被骗了XX钱，怎么能追回来？” “骗我的人抓得到吗？” “顺着网络查怎么就查不到人呢？”，“有银行卡、电话、网站信息，怎么躲在背后的人，就是抓不到呢？”

为什么骗子抓不到？

层层伪装的诈骗分子

第1层，地理伪装

大量丢失、被盗的第二代居民身份证，在网络黑市被公然叫卖。” 黑市，为诈骗分子提供了源源不断的身份信息资源。在普通人眼里，实名制是身份识别，但在诈骗分子眼中，实名制成为了规避风险的最佳手段之一。因为这些身份信息的所属人和诈骗分子压根没有关系。

第3层，技术伪装

专业洗钱集团主要服务于各类诈骗团伙，他们用最短的时间，将其他诈骗同行“辛辛苦苦”骗来的钱取出来，并用合法途径返还。将银行卡上的一串串数字变成能装在口袋里的真金白银。集团各个层级的人兢兢业业、分工合作、随时响应，形成了一张无形却又强大的蜘蛛网，只要一有资金触网，立即就会在这张网络的作用下消失得无影无踪。

诈骗洗钱集团内部分
工极其精细，一般分为五个层级。第一层称为“声佬”，

专门负责打电话、发信息、邮寄等工
作；第二层称为“接数佬”，
负责连接“声佬”和下一层；第三层称为“刷机佬”，
顾名思义就是负责刷
POS机，把钱刷到网上结算中心去；第四层是“卡佬”，
负责提供各种银行卡，分别自己转移
；第五层就是“取款仔”
，专门负责取钱，可以自己去取，也可以付费叫别人去取。

层级纪律严明。五个层级职责明确，纪律严明。跨级之间相互不认识也无联系，每个层级只能跟上一层对接，决不能也无法越级与上上层联系。这样，即使“取款仔”被抓，一般也很难问出上一级的人是谁、在哪，更无法抓到上上一层，最高一层级几乎就是毫无风险。

多路出击分散资金。比如“声佬”骗到20万，可以叫“接数佬”A处理10万，“接数佬”B处理十万；“接数佬”A又可以叫“刷机佬”A处理五万，叫“刷机佬”B处理五万；“刷机佬”A又可以叫“卡佬”A处理贰万五，叫“卡佬”B处理贰万五；“卡佬”A又可以叫“取款仔”A取一万，叫“取款仔”B取一万五。

错综复杂的“子孙账户”

诈骗分子在获得骗款时，第一时间需要做的事情就是安全地将所获赃款洗白，通过购买比特币这类数字货币，能够快速、安全的让钱款成功变身，并完美躲避法律的制裁。

比特币所采用的是一个去中心化的支付系统,已经脱离了传统的金融清算系统。它利用特殊手段将诈骗分子所拥有的相同额度的比特币在多个钱包地址之间跳跃，从而清除掉它原本的加密货币信息。想要追查最终的地址？可以，去深不见底的暗网上找吧。

银行卡、电话、网站信息都是假的，办案民警斗智斗勇的程度，远超过你的想象，所以保护好自己“钱袋子”的最好方法，不是等着咱们民警去破案，而是提高防骗意识。

公安部门发布了最全60种典型网络诈骗手段
，这些都是血汗钱堆出来的案例，请所有人赶紧查收，尤其是一定要发给自己的父母，他们是被骗的主要人群。

一、仿冒身份欺诈

1、冒充领导诈骗:犯罪分子假冒领导等身份打电话给基层单位负责人，以推销书籍、纪念币等为由，让受骗单位先支付订购款、手续费等到指定银行账号。

2、冒充亲友诈骗:利用木马程序盗取对方网络通讯工具密码，截取对方聊天视频资料后，冒充该通讯账号主人对其亲友以“患重病、出车祸”等紧急事情为名实施诈骗

3、冒充公司老总诈骗:犯罪分子通过打入企业内部通信群，了解老总及员工之间信息交流情况，通过一系列伪装，再冒充公司老总向员工发送转账汇款指令。

4、补助金、救助金、助学金诈骗:冒充教育、民政、残联等工作人员，向残疾人员、学生、家长打电话、发短信，谎称可以领取补助金、救助金、
助学金，要其提供银行卡号，指令其在取款机上将钱转走。

5、冒充公检法电话诈骗:犯罪分子冒充公检法工作人员拨打受害人电话，以事主身份信息被盗用、涉嫌洗钱、贩毒等犯罪为由，要求将其资金转入国家账户配合调查。

6、伪造身份诈骗:犯罪分子伪装成“高富帅”或“白富美”，加为好友骗取感

情和信任后，随即以资金紧张、家人有难等各种理由骗取钱财。

7、医保、社保诈骗:犯罪分子冒充医保社保工作人员，谎称受害人账户出现异常，之后冒充司法机关工作人员以公正调查、便于核查为由，诱骗受害人向所谓的安全账户汇款实施诈骗。

8、“猜猜我是谁”诈骗:犯罪分子打电话给受害人，让其“猜猜我是谁”，随后冒充熟人身份，向受害人借钱，一些受害人没有仔细核实就把钱打入犯罪分子提供的银行卡内。

二、购物类诈骗

9、假冒代购诈骗:犯罪分子假冒成正规微商，以优惠、打折、海外代购等为诱饵，待买家付款后，又以“商品被海关扣下，要加缴关税”等为由要求加付款项实施诈骗。

10、退款诈骗:犯罪分子冒充淘宝等公司客服，拨打电话或者发送短信，谎称受害人拍下的货品缺货，需要退款，引诱购买者提供银行卡号、密码等信息，实施诈骗。

11、网络购物诈骗:犯罪分子通过开设虚假购物网站或网店，在事主下单后，便称系统故障需重新激活。后通过QQ发送虚假激活网址，让受害人填写个人信息，实施诈骗。

12、低价购物诈骗:犯罪分子发布二手车、二手电脑、海关没收物品等转让信息，当事主与其联系，以缴纳定金、交易税手续费等方式骗取钱财。

13、解除分期付款诈骗:犯罪分子冒充购物网站的工作人员，声称“由于银行系统错误”，诱骗受害人到ATM机前办理解除分期付款手续，实施资金转账。

14、收藏诈骗:犯罪分子冒充收藏协会，印制邀请函邮寄各地，称将举办拍卖会并留下联络方式。一旦事主与其联系，则以预先缴纳评估费等名义，要求受害人将钱转入指定账户。

15、快递签收诈骗:冒充快递人员拨打事主电话，称其有快递需签收但看不清信息，需事主提供，随后送“货”上门。事主签收后，再打电话称其已签收须付款，否则讨债公司将找麻烦。

三、活动类诈骗

16、发布虚假爱心传递:犯罪分子将虚构的寻人、扶困帖子以“爱心传递”方式发布在网络上，引起善良网民转发，实际上帖内所留联系电话是诈骗电话。

17、点赞诈骗:犯罪分子冒充商家发布“点赞有奖”信息，要求参与者将姓名、电话等个人资料发至社交平台上，套取足够的个人信息后，以获奖需缴纳保证金等形式实施诈骗。

四、利诱类欺诈

18、冒充知名企业中奖诈骗:冒充知名企业，预先大批量印刷精美的虚假中奖刮刮卡，投递发送，后以需交个人所得税等各种借口，诱骗受害人向指定银行账号汇款。

19、娱乐节目中奖诈骗:犯罪分子以热播栏目节目组的名，义向受害人手机群发短消息，称其已被抽选为幸运观众，将获得巨额奖品，后以需交保证金或个人所得税等各种借口实施诈骗。

20、兑换积分诈骗:犯罪分子拨打电话，谎称受害人手机积分可以兑换，诱使受害人点击钓鱼链接。如果受害人按照提供的网址输入银行卡号、密码等信息后，银行账户的资金即被转走。

21、二维码诈骗:以降价、奖励为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒。一旦扫描安装，木马就会盗取受害人的银行账号、密码等个人隐私信息。

22、重金求子诈骗:犯罪分子谎称愿意出重金求子,引诱受害人上当，之后以缴纳诚意金、检查费等各种理由实施诈骗。

23、高薪招聘诈骗:犯罪分子通过群发信息，以月工资数万元的高薪招聘某类专业人士为幌子，要求事主到指定地点面试，随后以缴纳培训费、服装费、保证金等名义实施诈骗。

24、电子邮件中奖诈骗:犯罪分子通过互联网发送中奖邮件，受害人一旦与犯罪分子联系兑奖，犯罪分子即以缴纳个人所得税、公证费等各种理由要求受害人汇钱，达到诈骗目的。

五、虚构险情欺诈

25、虚构车祸诈骗:犯罪分子以受害人亲属或朋友遭遇车祸，需要紧急处理交

通事故为由，要求对方立即转账。

26、虚构绑架诈骗:犯罪分子虚构事主亲友被绑架，如要解救人质需立即打款到指定账户并不能报警，否则撕票。

27、虚构手术诈骗:犯罪分子以受害人子女或父母突发疾病需紧急手术为由，要求事主转账方可治疗。

28、虚构危难困局求助诈骗:犯罪分子通过社交媒体发布病重、生活困难等虚假情况，博取广大网民同情，借此接受捐赠。

29、虚构包裹藏毒诈骗:犯罪分子以事主包裹内被查出毒品为由，要求事主将钱转到国家安全账户以便公正调查，从而实施诈骗。

30、捏造淫秽图片勒索诈骗:犯罪分子收集公职人员照片，使用电脑合成淫秽图片，并附上收款账号邮寄给受害人进行威胁恐吓，勒索钱财。

31、虚构外遇流产做手术:犯罪分子冒充儿子发送短信给父母，充分利用老年人心疼儿子的特点，诱惑受害者转账。

六、日常生活消费欺诈

32、冒充房东短信诈骗:犯罪分子冒充房东群发短信，称房东银行卡已换，要求将租金打入其他指定账户内。

33、电话欠费诈骗:犯罪分子冒充通信运营企业工作人员，向事主拨打电话或直接播放电脑语音，以其电话欠费为由，要求将欠费资金转到指定账户。

34、电视欠费诈骗:犯罪分子冒充电工作人员群拨电话，称以受害人名义在外地开办的有线电视欠费，让受害人向指定账户补齐欠费。

35、购物退税诈骗:犯罪分子事先获取到事主购买房产、汽车等信息后，以税收政策调整可办理退税为由，诱骗事主到ATM机上实施转账操作。

36、机票改签诈骗:犯罪分子冒充航空公司客服，以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

37、订票诈骗:犯罪分子制作虚假的网上订票公司网页，发布虚假信息,以较低票价引诱受害人上当。随后，以“订票不成功”等理由要求事主再次汇款，实

施诈骗。

38、ATM机告示诈骗:犯罪分子预先堵塞ATM机出卡口，并粘贴虚假服务热线，诱使用户在卡“被吞”后与其联系，套取密码，待用户离开后到ATM机取出银行卡,盗取用户卡内现金。

39、刷卡消费诈骗:犯罪分子以银行卡消费可能泄露个人信息为由，冒充银联中心或公安民警设套，套取银行账号、密码实施犯罪。

40、引诱汇款诈骗:犯罪分子以群发短信的方式直接要求对方向某个银行账户汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，往往未经核实，即把钱款打入骗子账户。

七、钓鱼、木马病毒类欺诈

41、伪基站诈骗:犯罪分子利用伪基站向广大群众发送网银升级、10086 移动商城兑换现金的虚假链接，一旦受害人点击后便在其手机上植入获取银行账号、密码和手机号的木马，从而实施犯罪。

42、钓鱼网站诈骗:犯罪分子以银行网银升级为由，要求事主登录假冒银行的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施诈骗。

八、其他新型违法类欺诈

43、校讯通短信链接诈骗:犯罪分子以“校讯通!的名义，发送带有链接的诈骗短信，一旦点击链接进入后，手机即被植入木马程序，存在银行卡被盗刷的风险。

44、交通处理违章短信诈骗:犯罪分子利用伪基站等发送假冒违章提醒短信，此类短信包含木马链接，受害者点击之后轻则群发短信造成话费损失，重则窃取手机里的银行卡、支付宝等账户信息，随后盗刷银行卡。

45、结婚电子请柬诈骗:犯罪分子通过电子请帖的方式诱导用户点击下载后，就能窃取手机里的银行账号、密码、通信录等信息，进而盗刷用户的银行卡，或者给用户通讯录中的朋友群发借款诈骗短信。

46、专业技术性强。通过网络社交软件宣传手机APP，下载注册后有“客服”及“专家”进行指导操作。

47、金融交易诈骗:犯罪分子以证券公司名义，通过互联网、电话短信等方式散布虚假个股内幕信息及走势，获取事主信任后，又引导其在自身搭建的虚假交易平台上购买期货、现货，从而骗取事主资金。

48、办理信用卡诈骗:在媒体刊登办理高额透支信用卡广告，当事主与其联系后，以缴纳手续费、中介费等要求事主连续转款。

49、贷款诈骗:犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以预付利息、保证金等名义实施诈骗。

50、复制手机卡诈骗:犯罪分子群发信息，称可复制手机卡，监听手机通话信息，不少群众因个人需求主动联系嫌疑人，继而被对方以购买复制卡、预付款等名义骗走钱财。

51、虚构色情服务诈骗:犯罪分子在互联网上留下提供色情服务的电话，待受害人与之联系后，称需先付款才能上门提供服务，受害人将钱打到指定账户后发现被骗。

52、提供考题诈骗:犯罪分子针对即将参加考试的考生拨打电话，称能提供考题或答案,不少考生急于求成，事先将好处费的首付款转入指定账户，后发现被骗。

53、盗用账号、刷信誉诈骗:犯罪分子盗取商家社交平台账号后，发布“诚招网络兼职，帮助淘宝卖家刷信誉，可从中赚取佣金”的推送消息。受害人按照对方要求多次购物刷信誉，后发现上当受骗。

54、冒充黑社会敲诈类诈骗:犯罪分子先获取事主身份、职业、手机号等资料，拨打电话自称黑社会人员，受人雇佣要加以伤害，但事主可以破财消灾，然后提供账号要求受害人汇款。

55、公共场所山寨Wifi:在公共场合放出钓鱼免费WiFi,当事主连接上这些免费网络后，通过流量数据的传输，将手机里的照片、电话号码、各种密码盗取，对机主进行敲诈勒索。

56、捡到附密码的银行卡:犯罪分子故意丢弃带密码的银行卡，并标明了“开户行的电话”，利用了人们占便宜的心理诱使捡到卡的人拨打电话“激活”这张卡，并存钱到骗子的账户上。

57、账户有资金异常变动:窃取受害者网银登录账号和密码，制造银行卡上有资金流出的假象。然后假冒客服要求受害者提供自己手机收到的验证码来进一步诈骗 。

58、先转账、再取现、后撤销:犯罪分子利用银行转账新规中转账和到账时间的“时间差”来设置圈套。采取先转账、后给现金的诈骗套路，在骗取到受害人现金后，撤销转账。

59、补换手机卡:先用几百条垃圾短信和骚扰电话轰炸手机，以掩盖由10086客服发送到手机号码上的补卡业务提醒短信;然后，拿着张有受害者信息的临时身份证，去营业厅现场补办手机卡，使得机主本人的手机卡被动失效，从而接收短信验证码把绑定在手机APP上的银行卡的钱盗走。

60、换号了请惠存:犯罪分子通过非法渠道获得机主的通讯录资料后，假冒机主给手机里的联系人发短信，声称换了新号码，然后向其手机里的联系人进行诈骗。

宣传千万次，从不认真看。

骗后急报案，天天催破案。

骗子在境外，警察也为难。

破案要条件，防范是关键。

源头被阻断，哪里会被骗。

信息多转发，人人当宣传。

（来源：江苏刑侦）