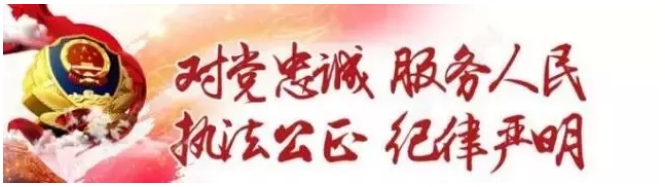
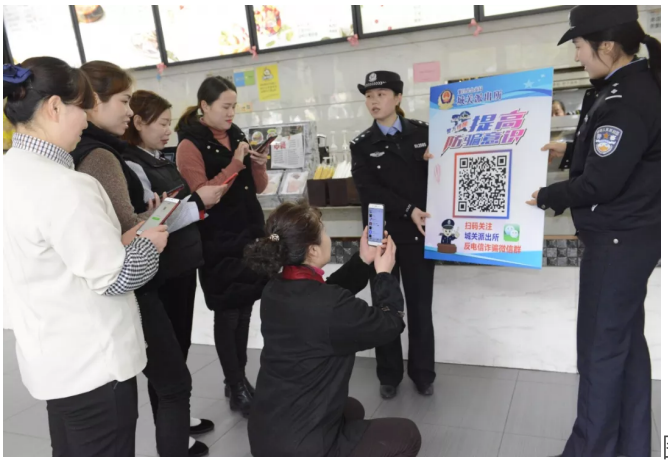
【防骗攻略】电信诈骗新“套路”，咱得认清了！

平安芜湖　3天前





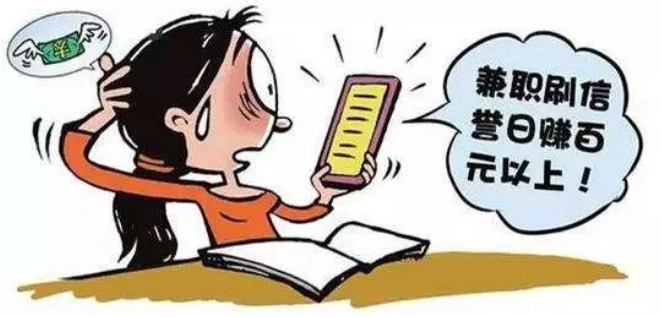
图为民警向某企业员工介绍“防范电信诈骗微信群”的使用

为压降电信诈骗案发生、防范群众财产损失，近日，繁昌县公安局城关派出所建立防范电信诈骗微信群，广泛吸纳辖区群众入群，常态化开展防范电信诈骗宣传。

电信网络诈骗犯罪持续多发高发，手段日益复杂，骗术层出不穷，让无数受骗者蒙受巨大损失，严重影响人民群众安全感。近几年，公安机关频频出手，打掉了一个又一个电信诈骗犯罪团伙，但电信诈骗仍时常发生。提高全民防范意识，是压缩电信网络诈骗犯罪的重要一环——

网上兼职刷单诈骗

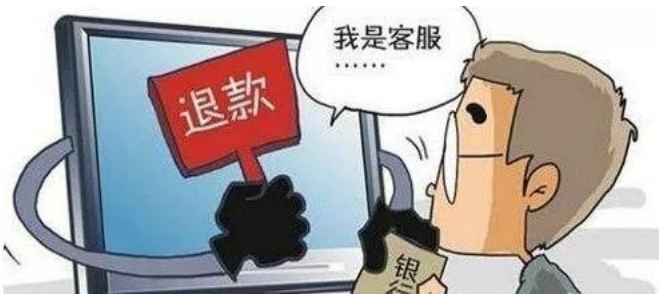
这类诈骗侵害的对象主要是大学生，骗子利用大学生思想单纯，没有社会经验，又迫切希望找到赚钱途径的心理实施诈骗。此类骗术让大学生还未走向社会就蒙上了心理阴影，影响恶劣。



骗子通过短信、QQ群或微信发布兼职刷单信息，要求接单者自己购买刷单商品，也就是在网上买商品，但不实际发货，许诺做任务刷单后返还本金并给予佣金。当接单者做完第一单任务后，骗子会按照许诺返还本金，并兑现小额佣金，以取得接单者的信任。当接单者继续付款刷单时，骗子会使出各种手段，增加其刷单购物数量和金额，接单者在付出这些钱后，骗子既不退本金也不付佣金。当接单者要求退还本金时，骗子便谎称系统故障，编造超时、任务未完成、卡冻结等各种理由让接单者继续付款刷单，等接单者发现被骗时，骗子瞬间就将接单者拉黑。随后，骗子利用接单者被骗后急于追回钱款的迫切心理，在网上设置“支付宝服务平台窗口”之类的假网站、QQ号、假客服电话，对接单者进行二次诈骗。当接单者向虚假的“支付宝服务平台窗口”投诉时，骗子称已冻结了账户，并提供冻结资金截图。当接单者要求转账退款时，骗子称接单者信用额度低，退款不成功，要接单者在支付宝上开通贷款来提高信用额度，并要接单者从支付宝内借钱转到指定账户验资，再次骗取接单者。

冒充淘宝客服诈骗

这类骗术主要侵害对象是喜欢网上购物的“剁手党”，主要是利用很多网购者不知道支付宝贷款功能的操作过程，稀里糊涂将从支付宝里贷款的钱转账到了骗子的账户上。



骗子通过非法渠道获取网购者的购物信息后，冒充淘宝客服以支付不成功，或者所购商品有质量问题需退款等理由，打电话给网购者，声称要将购物款退给网购者，不明真相的网购者往往认为这是陶宝服务的诚信所在，因而丝毫没有戒心，就按照骗子指导的步骤，操作起了支付宝的贷款功能，当贷出的款项到账后，网购者误认为这是收到的退货款，这笔款项肯定大于网购者支付的实际购物款，随后，骗子以多转了款为由让购物者退款，并给购物者发来二维码，让购物者扫描，善良的购物者根本不知道自己扫描的是支付码，最终将支付宝里的钱和从支付宝平台里贷款来的钱全部转到了骗子的账户上。

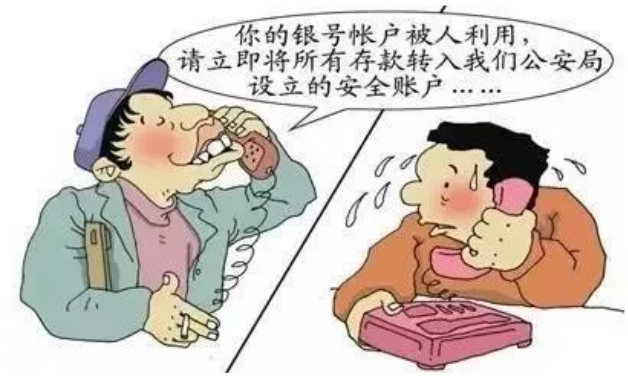
冒充企业领导诈骗

这类骗术侵害的对象主要是企业财务人员，主要是利用企业财务制度不完善，仅凭领导在QQ或者微信中发出的指令，就汇出巨额现金，这种诈骗非常普通，危害极大，轻则让企业“伤筋动骨”，重则使企业濒临破产。

这里常见的有两种作案手段：一是骗子通过“黑客”手段卧底到某公司群，植入木马，窥探公司聊天信息，搞清群内成员上下级关系，在半夜时将领导踢出群，或者临时组建包括财务人员在内的小群，骗子则用公司领导头像加入，使财务人员误认为骗子就是企业领导，受其指令打款；二是骗子通过网上搜索某公司信息，详细了解公司的经营财务情况和招聘信息，获得人事经理信息，通过QQ、微信冒充领导加其为好友，再编造出差等理由向人事经理获取公司通讯录，让人事经理通知财务加其QQ、微信，使财务人员深信不疑而听其指令打款。这类骗子在要求汇款前，一般都要发信息询问财务账户有多少可动用资金，当得到回复后，就告诉财务人员准备多少资金，一会需要用。在一切准备妥当后，骗子就会向财务人员发出信息，要求其从公司账户上转账到某某账户，达到诈骗目的。

冒充执法人员诈骗

这类骗术没有特定的侵害对象，具有很强的随意性，骗子主要利用公、检、法的执法威信，以涉案为由威胁、恐吓群众，让群众按照骗子的要求将银行卡、支付宝上的钱转帐到所谓的安全账户上。

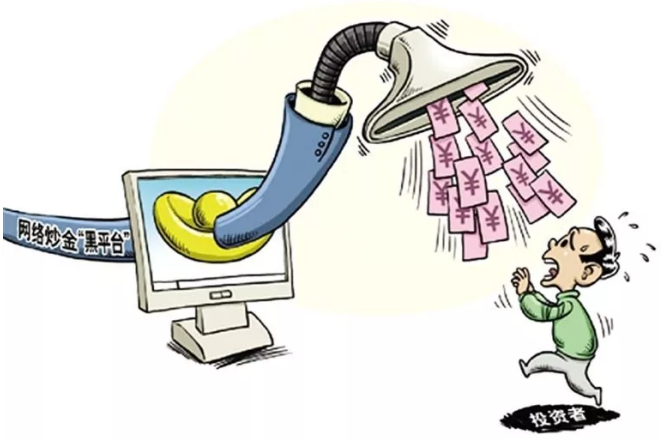


骗子随机拨打固定电话或者手机，发送储存的语音信息，并提醒需要咨询按人工服务键，当接电话的群众按人工服务后，骗子冒充邮政局、社保局、移动公司、银行等单位，称其办理了相关业务，恐吓其可能涉嫌犯罪，煞有介事地称公安机关正在调查，同时提供公安局电话（一般以上海、武汉等地公安局居多），随后，骗子通过改号软件将所用的电话号码改成公安局电话号码，冒充公安局、检

察院、法院执法人员先后打来电话，轮番轰炸式威胁，以涉嫌洗黑钱、贩毒等犯罪，让接电话的群众开宾馆或到一个安静的地方听其指示，同时要求其保密，不要对任何人说，对其做电话笔录，并恐吓受害人，获取其真实身份信息、银行卡信息，最后，要求接电话的群众按其指令到银行ATM机或网银、支付宝上操作，将自己账户里的钱转到所谓的安全账户上，行骗得手。

瞄准金融平台诈骗

这类诈骗主要针对的是股民和期货投资者，骗子利用投资者赚钱心切的暴富心理，通过QQ或者微信将其投资拉到非法投资平台，导致投资者血本无归。



骗子利用经各省级政府正式批准的一些现货交易平台发布信息，自称是其代理或加盟商，为其犯罪披上合法外衣。然后，通过短信、QQ群或微信招揽客户，当确定目标后，骗子就声称有指导老师指导操作，不仅不可能亏损，而且投资回报率高，以现货平台为幌子进行非法期货操作。在骗子甜言蜜语的狂轰滥炸下，有些人抵挡不住诱惑，开始试探性地进行小额投入，此时，骗子为了获取更大的利益，一般都会让投资者先尝到甜头，操控平台让其获利。但是，当客户加大投资后，骗子就原形毕露，他们通过收取手续费、反向操作、止盈不止损等方式将客户肆意宰杀。

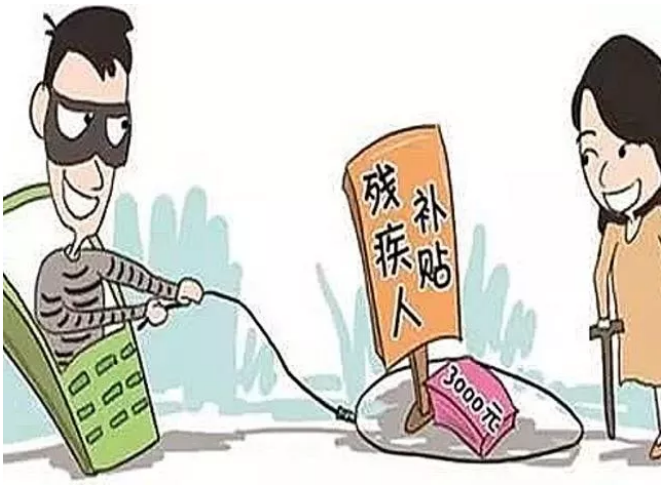
预测中奖信息诈骗

这类骗术完全针对期待天上掉馅饼的彩民，骗子利用彩民中大奖无门，急切希望预测到中奖号码的心理，发布虚假的能够预测到中大奖的信息，并要求彩民交纳会费注册，达到行骗目的。

骗子通过网络和各种交友软件，发布能够预测到彩票中大奖的虚假信息，当有彩民与其联系时，骗子会编造某某通过他们预测中了百万大奖。这些丝毫经不起推敲的谎言，有的彩民竟深信不疑。一旦彩民上钩，骗子会发送一个网站连接，彩民点击进入后，骗子提出预测彩票中奖号码必须成为网站的注册会员，有的彩民不加思考地按照骗子要求交纳注册费后，发现不能预测号码提出疑问时，骗子又以新会员必须充值激活，让彩民再次交费充值，一心期待中奖的彩民竟然毫不怀疑的照做，直到交出数千元，甚至上万元后，发现仍然无法获得中奖号码，才发现受骗，但为时已晚。

瞄准惠民政策诈骗

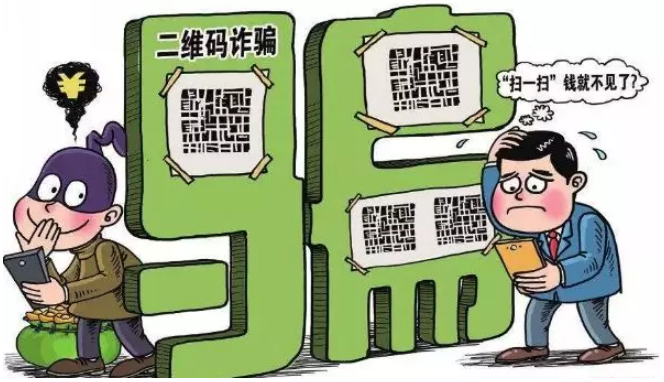
这类骗术主要针对刚录取的大学生和购车、生育、残疾等特定人群，骗子利用窃取到的特定人群信息，在惠及对象尚不了解如何兑现时，冒充当地干部，主动与惠及对象联系行骗。



针对这些特定人群在当前发生的事，骗子冒充政府有关部门的工作人员，打电话给他们，谎称政府对他们有补贴。接到电话的群众，听到是政府干部打来的电话，加上是发放补贴，一般都不会多想，就按照骗子的要求到银行ATM机上按其指令操作，结果不但没有拿到虚无的补贴，而且连银行卡里的存款也被骗子转走。2017年山东刚接到大学录取通知书的女孩徐玉玉受骗致死案就是个典型例子。

手机支付扫码诈骗

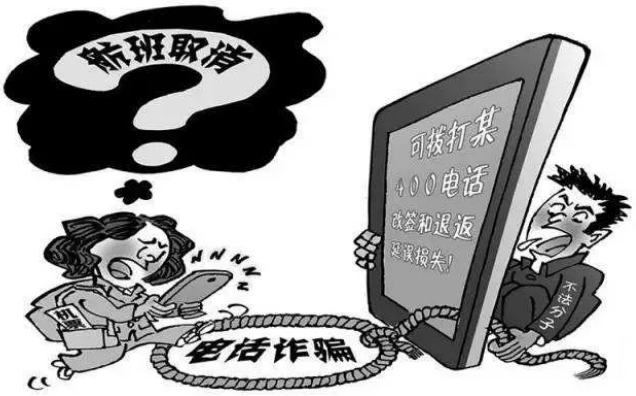
这类骗子侵害的对象主要是手机支付一族，他们利用收款码和付款码无法用肉眼识别的天然缺陷，让购物者在不知不觉中走进了圈套，这种诈骗数额虽然不大，但带有非常大的普遍性。



当前，手机支付已被广泛使用，骗子在群众订外卖或者购买商品时，以网络平台支付出现问题，无法接收付款等理由，诱使接受外卖订餐或者购物者使用骗子发来的二维码付款，骗子声称发来的是收款码，即付款人扫码后填写具体金额，再使用密码才能完成支付，但殊不知骗子发来的根本不是收款码而是付款码，主动权完全掌握在骗子手上，骗子通过千元以内小额免密支付方式盗刷付款人支付宝或微信账户资金，而付款码和收款码根本无法凭肉眼识别。这种骗术提醒我们，在使用扫码支付时，切不可轻易相信对方，尤其是陌生人，尽量不要使用这种自己没有控制能力的支付方式，以防止上当受骗。

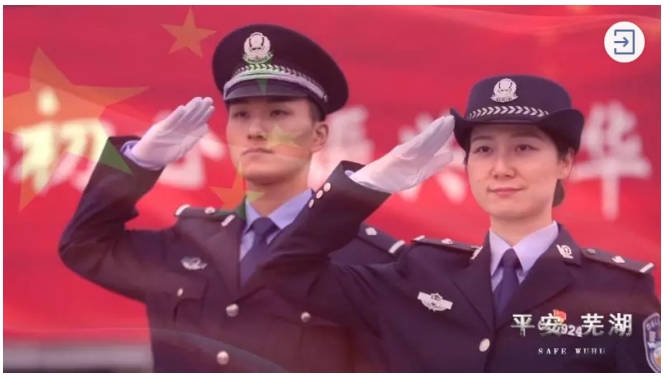
冒充航空客服诈骗

这类骗子侵害的对象是已经购买飞机票的乘客，他们通过非法渠道精确掌握了乘客信息，然后以航空公司客服的身份出现，编造飞机延误等理由，让乘客按照其指导获取退票费，结果将乘客银行卡里的存款转到了骗子账户上。



骗子通过非法渠道获得已经购买了机票的乘客信息，随后冒充航空公司客服，发送短信或者直接打电话给购买机票的乘客，称其所订的航班因机械故障或者其它问题不能按时起飞，请及时联系客服。乘客收到此信息后，几乎没有人能想到是骗子所为，因为骗子精准地说出了他们所乘航班的时间和起落地点，不是航空公司客服，别人怎么可能知道这些情况呢？因此，他们几乎是百分之百拨打客服电话号码，此时，骗子谎称要给乘客补偿误机费，要乘客在支付宝上根据其指导操作，其声称操作的退补偿费过程，实际是将乘客支付宝上的现金转出的过程，但由于乘客操作细节不了解，很难识破骗子精心设下的骗局，直到支付宝里的钱消失后才如梦方醒。

编辑：小薇



平安芜湖

我是特警支队 白甫

我在关注【平安芜湖】

别看啦，跟随警草脚步吧

平安芜湖