



防骗全民行



山东省反电信网络诈骗中心



请大家积极关注“山东反诈骗中心”微信公众号



山东省公安厅 编
山东省反电信网络诈骗中心

防骗十讲

电信网络诈骗是不法分子通过电话、网络 and 短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗。那么生活中常见的电信网络诈骗手法有哪些？它们的具体实施过程是怎样的？遇到各类诈骗，你是否能提高警惕，避免上当？今天，我们来一起学习电信网络诈骗的相关知识吧~





防骗讲堂第一讲 刷单诈骗

5月的一天,市民王女士在家里玩QQ时,添加了一个号称能兼职赚钱的QQ群。她一加入这个QQ群,一个昵称为“客服001”的人便热情的联系她,并告诉她可以提供一份刷单兼职的工作,能赚不少钱!在介绍了刷单兼职方式后,王女士认为简单易操作,便答应参与刷单,于是对方发给她一个支付宝收款的二维码。王女士通过支付宝扫描二维码向对方支付100元,后对方返还其本金+佣金总计105元。

第一单成功了,消费了100元的本金,5分钟对方返款105元,在收回本金的基础上还赚了5块钱,王女士感到很满意,又进行了第二单。就这样,一次次的成功,让她渐渐地开始信任对方,虽然期间也曾产生过一丝怀疑,但是客服给她发来了各种所谓的本公司



证件,且这些证件全部在网络可以查询到,于是王女士彻底打消了疑虑,以扫描二维码的支付方式多次刷单共计3万余元。随着金额的累积,对方并没有如之前一样快速返款,而是以各种理由让王女士继续刷单,当对方发现王女士觉察到不对劲不想再继续刷单时,就把她拉黑了。



民警提示:

刷单本是不合规不合法的行为,它危害市场秩序,侵害消费者权益,更成为了犯罪分子实施诈骗的手段。我们要远离这些打着“工作轻松,报酬丰厚”旗号的刷单行为,坚决不相信天上掉馅儿饼的事!



防骗讲堂第二讲 冒充银行客服诈骗（一）

市民莫先生收到了一条短信，短信上说因莫先生的信用卡出现了逾期还款，现在已被冻结，并且进入黑名单，如需恢复请致电0086156XXXX0532（XX银行）。

莫先生看到号码，认为是银行官方客服发送的短信，应该没有问题，便按照短信上的号码打电话进行询问。电话接通后，一位自称是银行工作人员的人询问莫先生，为什么信用卡会出现逾期，莫先生告诉客服是他忘记还款了。随后该客服便告知莫先生为了让其还款方便有保障，现需绑定莫先生名下的一张银行卡。



莫先生没有多想，便按照客服的指示告诉对方自己名下的一张工商银行卡号、密码、以及自己的身份证号码，随后对方又在电话里三次向莫先生索要发到其手机上的验证码，莫先生把验证码告知对方后，卡内的10万元就被转走了。



民警提示:

收到类似短信千万不要轻信，更不能拨打短信中所留的客服号码。正规银行不会在业务办理提醒短信中让用户拨打非银行的客服电话，银行工作人员在办理业务的过程中，也不会索取用户的密码和动态验证码。



防骗讲堂第三讲 冒充银行客服诈骗（二）

9月中旬，大学生小张接到一个自称淘宝公司工作人员的电话，对方称因员工操作失误，将100多名客户误设为至尊会员，其中就有他的帐户。成为至尊会员，每月将扣款600元，一年算下来年费就是7200元。对方电话里问小张是不是自愿的，作为家里没矿的学生竟小张当然否认，接着对方又说他可以帮忙取消该会员，但是需要小张开具回款单等证明。

小张回忆说，当时他也没有听明白，对方就把电话给他转接到了“中国农业银行”。“银行接线员”问小张怎么回事，他就按照之前淘宝工作人员教给自己的话复述了一遍“我是XX，我要取消淘宝至尊会员，因为不是我本人办理的而是员工失误，请给我一份回款单。”

“银行”接线员说，小张可以选择去附近银行办理取消会员或由接线员在线办理，并开具电子回款单。小张选择了自行去附近分行办理……接着“接线员”就把电话挂掉了……

这时，之前的“淘宝工作人员”又出现了，他质问小张为什么银行方面把会员取消申请单退回来了？小张就把之前的情



况说了一下，这名“工作人员”说因为银行退回申请，淘宝方面将会连夜在帐户扣款。小张一听着急了，由于附近银行已经下班了，只能让对方转接银行选择在线办理业务。

“银行接线员”让小张通过微信，将卡里的7200元转入了指定帐户，美其名曰帮助他暂时代管以避免其损失，小张害怕淘宝真的给她扣款呀，赶紧按对方的要求把钱转了过去……

后来，小张回想整个过程才明白自己是被骗了，赶紧去公安机关报了警。



民警提示：

接到网络平台客服电话要多方核实，一定要通过网站官方联络工具，切忌跳出原有平台进行交易。坚决不扫对方发来的二维码，不随意填写私密信息，不轻易向他人账户转账。



防骗讲堂第四讲 中奖诈骗

市民王先生收到一条某网站发来的中奖短信，短信上说该网站双十一特别策划，回馈新老客户举行抽奖活动，王先生荣获二等奖，奖金10万元，请其速与兑奖中心经理联系领取。王先生立刻拨打了短信上留下的电话，对方给他提供了一个银行卡号，称要想领奖需支付5000元的公证费，完成公证之后即可支付奖金。为了即将到手的10万元钱，王先生给对方汇去了5000元公证费，但对方并没有立即支付奖金，而是又连续以手续费、交税等名义，多次要求王先生汇款，而且称王先生不接着汇款，之前交上的钱款也无法返还。

您中奖了，只要支付5000元的公证费，10万奖金就是您的了！



王先生只得按照对方要求支付了各种费用后，但是最后没有收到所谓的奖金。



民警提示：

接到任何红包、中奖信息一定要提高警惕！多方核实其真伪，坚决不点击陌生链接，不扫描陌生二维码。不要被虚无的利益所迷惑，千万捂好自己的钱袋子！



防骗讲堂第五讲 网络购物诈骗

一、低价购物

刘先生爱好收藏工艺品，有朋友介绍的、有主动添加他的，不知不觉微信里有了很多卖工艺品的好友，刘先生也会偶尔刷刷朋友圈，看看有没有心仪的物件。这天，他看到一位不什么时候加上的微信好友在朋友圈发了几件木雕作品，他一眼就看上了，便主动跟这位好友询价，经过一番讨价还价，双方约定以2万多元的价格成交，但是刘先生要全额付款后对方才能发货。开始刘先生有点担心，但价格比较优惠，再加上对方一再保证自家店铺都是这样的，从来没出问题，而刘先生自己实在喜欢，便给对方汇了款。可自从付款后，这位卖家却并没有按照约定发货，而是以商品有质量问题等借口迟迟不给发货，后来干脆拉黑了刘先生消失不见了。



二、预售购物

市民林小姐眼见“双十一”快来了，早就关注起各家淘宝店的活动动态。当天，她的手机收到一条陌生号码发来的短信。“11.11提前购、剁手价、包邮”等字眼映入眼帘。林小姐想都没想便点了短信里的链接。手机界面跳转后，卡在空白页就不动了。林小姐以为手机出了故障，就关机重启。手机开机后，接连几条银行短信轰炸，让她顿时傻了眼。就在她关机期间，银行卡里被转走3笔钱，共计3000元。原来，林小姐点击的是木马链接，病毒迅速侵入手机，盗获其绑定在购物平台的银行帐户。



民警提示：

通过转账或红包的方式支付全部货款或一定数额的定金，再由买家发货，没有平台监督，存在很大的风险，大家因尽量选择正规购物网站购买商品，这也是给自己提供了多一层的保障。收到各种优惠链接，可以向官方客服咨询真伪，不要轻易去点击这些链接，更不要在链接中输入任何个人信息！同时，请给手机装上杀毒软件，提供安全的上网环境。



防骗讲堂第六讲 网络投资诈骗

一天，李某在微信上收到了一条好友信息，这位好友没有备注名，也不知是什么时候加上的。对方称自己是一个炒股专家，有25年的从业经历，对股市预测精准，还给他看了自己进行股票分析的视频。问李某有没有兴趣跟着自己一起炒股。通过跟这位微信好友的交流，李某认为他懂得很多炒股知识，果真是个专家，就跟着他一起炒股了。一个月之后，“专家”告诉李某现在股票市场动荡，炒股风险较大，建议把资金从股市退出来参与炒黄金。他自己有十多年炒黄金的经验，现在也在做这一块，利润很大，能实现翻倍。如果李先生有意向跟随自己炒黄金，可以加入一个微信群进行进一步的交流。李某随后便被拉入了一个微信群，这里有很多和自己一样参与炒黄金的“投资人”，还有几位“老师”和一名“客服人员”。

“老师”定期讲解炒黄金期货的知识，介绍着号称具有雄厚实力的投资公司。什么“波浪理论”呀“布林线法则”呀，各种各样的知识令李某感到受益匪浅。其他“投资人”也会积极回应，纷纷在群里公布自己投资了多少，收益了多少。客服人员更是天天给大家鼓劲，鼓励大家参与投资。

客服与李某和信交流，对方很耐心的给他讲解了开户的程序，安装软件的防范以及其他的相关手续。“专家”也现场给他演示过炒黄金的过程，让他亲眼见证了大额的盈利……李某注册了帐号，先后向平台转账20余万元，他每天根据专家在微信群里发送的信息入金出金，或涨或跌，每天虽少亏多，一个月后就只剩下千余元。这时的李某并没有意识到自己上当受骗，只是当做投资不当造成的亏损，但是当他想要再次充钱投资时，却发现无法操作。客服以银行升级、需要更换银行卡等理由进行解释，后来干脆不见了人影，李某才觉被骗。



其实，他是遇到了一个以炒黄金、炒期货为由实施诈骗的团伙，此类团伙分工明确，有所谓“投资分析师”、有“收益客户”还有“平台客服”等。他们通过微信群聊等方式诱骗客户进行投资，有的利用虚假交易故意把客户的钱都“做亏掉”，给客户造成投资失败的假象，有的等骗取一定数额的资金后直接关闭平台，令受害人血本无归。受害人根本不会知道，他们所在的这个投资微信群，里面除了他自己，都是分工不同的犯罪嫌疑人！他们制造的各种假象，不过是让受害人进行大额投资。



民警提示：

不要随意添加陌生人微信，可能会给未来个人信息安全等带来隐患；不要轻信所谓“投资专家”，更不要随意加入各种投资微信群，群里形形色色的人让你难辨真假。投资理财诈骗通常涉案金额较大，想要投资应当选择正规的渠道！



防骗讲堂第七讲 信用卡类诈骗

八月初的一天，市民小孙收到一条来自“XX银行”的短信，内容是“【XX银行】尊敬的用户你好：我行信用卡中心诚邀您提升卡片额度50000元，详情点击<http://xxxxxxx.com>申请。回T退订”，小孙正好想提高信用卡的额度，于是就点开链接。打开连接后，上面显示需要小孙重新填写个人信息。因为发件人显示的是银行的官方客服号码，小孙没有多想就把自己的身份证号码以及手机号码等个人信息填写了上去，并将收到的手机验证码也填写完成。之后，他很快便收到了短信，可短信显示的不是他提额成功，而是他的信用卡在外地消费7000余元的消费记录，这时候小孙才发现自己被骗了。

小孙这是中了诈骗分子的套路，常见的套路有以下

套路一：谎称信用卡证件资料过期

骗子通过发送短信的方式告知受害人的信用卡的证件资料已经过期，需要登录银行的网站进行更新，不然可能会影响正常使用，后面还有一个所谓的银行网站的链接，一旦点击该链接并按对方要求操作，银行卡的钱就会被盗刷。



骗术二：谎称信用卡可以提升额度

骗子还可能会仿照银行的短信，通过伪基站改号软件用和银行官方客服电话相同的号码发送短信：“我行根据您的信用率消费情况综合评分，现在可以提升百分之五十的额度，请在线申请。”后面也有个提升额度的网站地址，在填写了个人信息和验证码后，信用卡就会被盗刷。



民警提示：

以后收到类似的短信，不要轻易点开短信的链接，不要回拨短信中的电话，更不要随便泄露自己的个人信息。银行业务尽量到银行大厅办理以免上当受骗！



防骗讲堂第八讲 冒充子女诈骗

场景一

这天，张妈妈在QQ上收到一条申请添加好友的消息，对方自称是女儿王小宝，这是自己新注册的号码。过了一会儿，小宝给她发消息：“麻麻，清华大学资深老师来我们学校办培训班了，一门收费9900，很多同学都报了，名额有限，你快给我报名吧！”

场景二

这天，王先生也收到了儿子发来的QQ消息，清华大学的老师去他们学校办培训班，而且这培训班可不是谁都能参加的，除了一门9900的培训费，还要老师进行评估，只有优秀的学生才有机会！

清华大学+资深老师+名额有限=机会难得呀！！

尽管觉得价格有些贵了，但为了孩子的学业，这些投入是值得的！家长们还是把钱转给了孩子提供的培训班帐号。

可接下来，孩子们的学习热情犹如滔滔江水……报完语文报数学，报完数学报英语，一口气报了三四门功课，后来又要收取保证金……这时，家长才觉得不大对劲了，立刻与学校老师取得了联系，原来根本没有办培训班这一回事，他们这是遇到电信网络诈骗了！



现在我们来分析一下骗子的套路：首先，他们会发信息给受害人，过程大致如下：“妈妈（或爸爸），我是XXX，我的手机没电了或正在上课，不能用开机或新申请的号”；然后，这个XXX告诉妈妈（或爸爸）学校邀请到资深教授来校办培训班，机会难得，报名人数有限，自己也想参加；接着骗子会发来负责报名收费的学校老师的帐号或联系方式，让父母咨询并联系缴费；等家长汇完钱，可能认为没事了，骗局结束了，但没那么简单，很可能骗子还会与你联系，说钱已收到，但还需要缴纳其他费用等。



民警提示：

学生家长，遇到此类以孩子以学费、培训费等理由要求转账汇款的情况，一定要当面或采用电话、视频聊天的方式联系孩子核实情况。一旦无法和孩子取得联系，要及时联系学校和班主任老师，不要盲目汇款，以免落入诈骗分子的圈套。



防骗讲堂第九讲 冒充公检法诈骗

王某接到一通这样的电话：“你好，我是广州市公安局民警××，警号××××。请问你是不是王×，身份证号××××××××？”王某承认了自己的身份后，对方又说“经过调查，我们发现你的身份信息涉嫌拐卖儿童，如果不是你，那可能是犯罪嫌疑人使用了你的身份进行违法犯罪活动，现在需要对你名下的银行卡进行调查。”听到这里，王某着急了，急忙辩解道“不可能啊，绝对不是我干的！”这时，对方继续说“你现在只需要配合我们警方调查清楚，证明你的卡里不是违法犯罪所得就可以。你需要把你的银行卡里的存款转移到我们公安局的安全帐户，之后我们会对你的帐户进行核查。要是核查发现没有什么问题，钱再返还到你的原帐户。”于是，王某就按照对方的指示将资金汇入了帐户。

最近，还出现了“冒充公检法2.0”

2018年11月21日，于博士下班时接到10086电话称其名下手机卡涉嫌发送大量违法信息，后转到上海市公安局，然后民警让其加QQ进行语音通话，并通过QQ出示了大量证明和法律手续，于博士信以为真，被骗68万。

原来，在“2.0”版本中，骗子为了追求效果的逼真，会向受害人发送“警官证”的照片，并将所谓姓名、警号等信息告诉他们。

虽然，骗子在不断升级诈骗手法，但是换汤不换药，冒充公检法诈骗主要还是通过以下几个步骤：

第一步：骗取信任：骗子采取分工合作的方式，通过网络购买受害者个人信息后，先由专人告知你的手机卡，银行卡等方面存在问题，来取得受害者初步信任。随后帮你把电话转到某地公安局或国家机关，期间骗子还会通过改号软件将来电显示为警方办公电话，让受害人拨打114查询验证，进一步增强信任。



第二步：震慑：骗子会通过声色俱厉的声音，强势震慑并控制受害人。

第三步：恐吓：骗子让受害人彻底相信自己卷入了一个重大案件，随时可能被逮捕。为了增强恐吓，让骗局更加逼真，骗子甚至还会通过虚假政法机关或网络传真让受害人收到一份通缉令。

第四步：转账：利用受害人的恐慌心理，缓和语气，诱骗受害人入局。

第五步：电话遥控转账：骗子声称资金调查，实则是要求受害人把银行卡插入ATM机，然后把卡内的资金转到指定的帐户。



民警提示：

只要是涉及金钱，都应再三确认！公安机关不会通过电话做笔录的！“公检法”没有所谓的“安全账户”，更不会指导你转账。“安全账户”等于诈骗。请守住自己的钱袋，不要轻易向陌生人汇款！



防骗讲堂第十讲 贷款诈骗

市民刘女士接到一个陌生电话问其是否需要网络贷款，因近期确实需要用钱，在跟对方简单了解后，刘女士便添加了对方提供的QQ号为好友。

加上好友后，对方给刘女士发了一个二维码让其下载了一款名为“XX贷”的软件，刘女士在这个软件上注册了帐号并绑定了银行卡，同时申请了1万元的额度。

这时，对方告诉刘女士，如果想要快速通过申请，必须要转帐2000元作为押金，刘女士没有多想，立即通过银行卡向帐号内打入了2000元，打钱成功后，系统便显示贷款成功，但刘女士却始终无法提现，便联系对方进行询问，这时对方则称因财务下班，目前无



法提现，第二天才能到帐。就这样，刘女士一直等到了第二天晚上，钱却还是迟迟没有到帐，于是刘女士再次通过QQ试图联系对方，这时才发现，对方已将自己拉黑了。



民警提示:

不要轻易把自己的信息泄露到网贷平台，在提交自己的各种资料之前，一定要对网上的放贷平台进行一个仔细的考察，是否有固定的联系方式、固定的办公场所，以及是否在当地工商局注册。一上来就让先交钱的绝不可信，骗子为了能够快速骗到钱，往往一开始就会以各种名义让当事人交取各种费用，等当事人交费后发现自己被拉黑。