

# 警情通报

重点关注：2021年1-4月共发生诈骗案件47起，其中本科生以低年级为主，案件类型以冒充熟人、客服及网购诈骗为主，涉案金额小，但发案数量多；研究生以高年级为主，案件类型以消除网贷（分期消费）记录为主，发案量低但涉案金额高。

蜀黍家 SHUSHUJIA | 乌云君 WUYUNJUN

## 58种诈骗手法 9大类型

### 通讯网络诈骗之 仿冒身份

通讯冒充伪装成领导、亲友、机构单位等身份进行诈骗。

- 冒充秘书**

不法分子冒充上级领导秘书等身份打电话给下属单位负责人，以推销书籍、纪念币等为由，让受骗单位支付订购款、手续费等，实施诈骗活动。
- 冒充亲友**

不法分子在与人视频聊天时，截取对方画面，随后再利用木马程序等盗取对方信息，用视频画面冒充本人与亲友聊天，骗取信任后便以各种理由要求汇款实施诈骗。
- 冒充公司老总**

不法分子打入企业内部通讯群，了解领导及员工之间的信息，再通过伪装微信账号等，冒充领导对员工进行诈骗。
- 补助救助、助学金**

不法分子冒充教育、民政、残联等工作人员，向学生、市民、残疾人员打电话或发短信称可以领取相关补助或救助金，诱导受害人通过ATM机或其他途径汇款，从而实施诈骗。
- 冒充公检法电话**

不法分子冒充公检法工作人员，以事主身份信息被盗用、涉嫌犯罪等理由，要求受害人将其资金转入安全账户配合调查，以此实施诈骗。
- 伪造特定身份**

不法分子伪装成高富帅、白富美等，通过恋爱等方式骗取受害人的信任，随即以资金紧张家人有难等各种理由骗取钱财。
- 医保、社保**

不法分子冒充医保、社保工作人员，称受害人账户出现异常，诱骗受害人向所谓的安全账户汇款。
- “猜猜我是谁”**

不法分子打电话给受害人，让其“猜猜我是谁”，随后冒充熟人身份，以各种理由向受害人借钱。

### 通讯网络诈骗之 购物类

通过各种虚假优惠信息、客服退款、虚假网店等实施诈骗。

- 九 假冒代购**

不法分子以优惠、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”等理由要求继续付款，或索性拉黑不发货，从而实施诈骗。
- 十 退款**

不法分子冒充网店客服，拨打电话或者发送短信，谎称缺货，要给受害人退款，引诱购买者提供银行卡号、密码等信息，或扫描指定二维码，从而实施诈骗。
- 十一 网络购物**

不法分子开设虚假购物网站，在受害者下单后，便称系统故障需重新激活，发送虚假激活网址，让受害人填写个人信息，实施诈骗。
- 十二 低价购物**

不法分子通过发布二手车、二手电脑、海关没收物品等转让信息，以缴纳定金、交易税、手续费等为由骗取钱财。
- 十三 解除分期付款**

不法分子冒充购物网站工作人员，声称银行系统错误，谎称受害人被办理了分期付款等业务，诱骗受害人到ATM机前操作，利用英文界面等实施诈骗。
- 十四 收藏**

不法分子冒充收藏协会，印制邀请函邮寄各地，称将举办拍卖会并留下联系方式。一旦受害人与其联系，则以各种名义收费，要求受害人将钱转入指定账户。
- 十五 快递签收**

不法分子冒充快递人员联系受害人，称其有快递需签收但看不清信息，以此套取受害人信息。随后送货上门，签收后威胁受害人付款，否则将引来麻烦。

## 通讯网络诈骗之 **活动类**

通过微信、微博等社交工具发布各种虚假活动，引诱用户参与进行诈骗。

### 十六 发布虚假爱心传递

不法分子虚构寻人、扶贫、准考证丢失等爱心帖子，利用网民的善良和爱心骗取转发，实则帖内所留联系电话并非真实，甚至会通过电话或网页套取个人信息。

### 十七 点赞

不法分子冒充商家发布“点赞有奖”的信息，要求参与者提供姓名、电话等信息，不仅如此，套取足够的个人信息后，不法分子还会以获奖需缴纳保证金等理由要求受害人汇款。

## 通讯网络诈骗之 **利益诱惑类**

通过捏造各种意外不测、让用户惊吓不安的消息实施诈骗。

### 十八 冒充知名企业中奖

不法分子冒充知名企业，印刷大量虚假中奖刮刮卡，投递发送，一旦有人上当，便会以各种理由收取费用。

### 十九 娱乐节目中奖

不法分子以热播栏目节目组的名义向受害人群发短消息，称其已被抽选为幸运观众，将获得巨额奖品，后以缴纳保证金或个人所得税等借口实施诈骗。

### 二十 兑换积分

不法分子谎称受害人手机积分可以兑换奖品，诱使受害人点击钓鱼链接，一旦点击并填写信息，受害人的银行卡号、密码等信息将被套取。

### 二十一 扫描二维码

不法分子以降价、奖励为诱饵，让受害人扫描二维码加入会员或领取优惠，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、密码等个人信息。

### 二十二 重金求子

不法分子以重金求子为诱饵，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。

### 二十三 高薪招聘

不法分子通过各种途径群发信息，以高薪招聘等为幌子，要求受害人到指定地点面试，随后以缴纳培训费、服装费、保证金等名义实施诈骗。

### 二十四 电子邮件中奖

不法分子通过互联网发送中奖邮件，一旦有人上当，不法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款。

## 通讯网络诈骗之 **虚构险情类**

通过捏造各种意外不测、让用户惊吓不安的消息实施诈骗。

### 二十五 虚构车祸

不法分子谎称受害人亲友遭遇车祸，以需要紧急处理交通事故为由，让受害人转账。

### 二十六 虚构绑架

不法分子谎称受害人亲友被绑架，让受害人转账，并威胁不能报警，否则撕票。不法分子通常会选择工作时间给家里打电话，留守在家中的中老年人往往不知所措，容易上当受骗。

### 二十七 虚构手术

不法分子谎称受害人子女或父母突发疾病需紧急手术，要求事主转账方可治疗。受害人往往因为担心、心急便按照不法分子指示转账。

### 二十八 虚构危难困局求助

不法分子通过社交媒体发布病重、生活困难等虚假信息，博取广大网民同情，借此接受捐赠。

### 二十九 虚构包裹藏毒品

不法分子谎称受害人的包裹被查出毒品要求受害人将钱转到所谓的安全账户以便调查从而实施诈骗。

### 三十 合成照片勒索

不法分子通过各种途径收集受害人照片使用电脑合成为不良图片，并附上收款账号邮寄给受害人进行威胁恐吓，勒索钱财。

### 三十一 冒充特定对象

不法分子群发短信，并谎称自己与对方有特定关系，以怀孕等事由骗取钱财，利用巧合性以及“家丑不外扬”的心态，诱感受害者转账。

## 通讯网络诈骗之 **日常生活消费类**

针对日常生活种各种缴费、消费等实施诈骗。

### 三十二 冒充房东短信

不法分子冒充房东群发短信，谎称房东银行卡已换，要求将租金打入其他账户，部分租客不加以核实便信以为真，发现受骗时为时已晚。

### 三十三 欠费

不法分子冒充工作人员群拨电话，称受害人有水、电、煤等类型的欠费，让受害人向指定账户补齐欠费，部分群众信以为真，转款后才发现被骗。

### 三十四 购物退税

不法分子以购物可办理退税为由，诱骗受害人到ATM机上实施转账操作，利用英文界面等实施诈骗。

### 三十五 机票改签

不法分子冒充航空公司客服，以“航班取消、提供退票或改签服务”等理由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

### 三十六 订票

不法分子制作虚假的订票网页，发布虚假信息，以低价引诱受害人上当。随后以“订票不成功”等理由要求受害人再次汇款，实施诈骗。

### 三十七 ATM机告示

不法分子在ATM机出卡口做手脚，并粘贴虚假服务热线，使用户使用异常后与其联系，从而套取密码。

### 三十八 刷卡消费

不法分子以银行卡消费可能泄露个人信息为由，冒充银联中心或公检法设套，套取银行账号密码等信息。

### 三十九 引诱汇款

不法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，如果碰到恰巧需要汇款的受害人则很容易上当，往往不经核实，便轻易相信。

## 通讯网络诈骗之 **钓鱼、木马病毒类**

通过伪装成银行、电子商务等网站窃取用户账号密码等隐私的骗局。

### 四十 伪基站

不法分子利用伪基站冒充官方平台向用户发送网银升级、手机积分兑换等虚假信息，并在其中加入链接，一旦受害人点击便在其手机上植入木马获取个人信息，从而进一步实施诈骗。

### 四十一 钓鱼网站

不法分子以网银升级为由，要求被害人登录事先准备好的钓鱼网站，从而获取被害人的银行账户、网银密码等信息实施诈骗。

## 通讯网络诈骗之 提供特定服务类

谎称可以提供各类非法服务，以此实施诈骗活动。

### 四十二 交通处理违章短信

不法分子利用伪基站等发送假冒违章提醒短信，受害人一旦点击短信中的链接，即被植入木马病毒，轻则群发短信造成话费损失，重则会被窃取银行卡、电子账户等个人信息，造成巨大损失。

### 四十三 金融交易

不法分子以证券公司名义，谎称有内幕消息并通过互联网、电话、短信等方式散布，一旦有人上当，便引导受害人在他们搭建的虚假交易平台上的进行操作，以此骗取受害人资金。

### 四十四 办理信用卡

不法分子通过各种渠道散布广告，称可以办理高额透支信用卡，一旦有人相信，便会以各种理由要求受害人缴纳各种费用。

### 四十五 贷款

不法分子群发信息，称可以提供贷款，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。

### 四十六 复制手机卡

不法分子群发信息，称可复制手机卡，监听手机通话信息，受害人一旦相信，便会被对方以购买复制卡、预付款等名义骗走钱财。

### 四十七 虚构色情服务

不法分子通过各种方式散布提供色情服务的电话，受害人一旦与其联系，不法分子便称需先付款才能提供服务，而受害人一旦汇款，他们便会消失。

### 四十八 提供考题

不法分子会针对即将参加考试的考生拨打电话或发送短信，称能提供考题或答案，不少考生将钱转入指定账户后才发现上当受骗。

### 四十九 刷信誉

不法分子冒充商家发布招聘信息，称帮助卖家刷信誉，可从中赚取佣金。受害人按照对方要求多次购物刷信誉，之后却再也无法与他们取得联系，这时才发现上当受骗。

## 通讯网络诈骗之 其他新型违法类

谎称可以提供各类非法服务，以此实施诈骗活动。

### 五十 校讯通短信链接

不法分子以“校讯通”的名义，发送带有链接的诈骗短信，一旦点击链接，手机即被植入木马程序，存在银行卡被盗刷的风险。

### 五十一 结婚电子请柬

不法分子通过发送电子请帖，诱导用户点击下载，以此窃取银行账号、密码、通讯录等信息，进而盗刷银行卡，或者给通讯录中的亲友群发诈骗短信。

### 五十二 相册木马

不法分子冒充各种身份，引诱受害人点击电子相册，其中植入的木马病毒便会获取用户网银信息等。

### 五十三 冒充黑社会敲诈

不法分子自称黑社会，恐吓受害人称有人要对其加以伤害，但又称可以破财消灾，然后提供账号要求受害人汇款。

### 五十四 公共场所山寨WiFi

不法分子设置免费WiFi引诱用户连接，一旦连上，通过流量数据的传输，黑客就能轻松盗取手机里的照片、电话号码等信息，从而实施进一步

### 五十五 捡到附密码的银行卡

不法分子故意丢弃银行卡，并在其中附上密码，标明“开户行电话”，诱使捡到卡的人拨打电话“激活”并存钱到骗子的账户上。

### 五十六 账户有资金异常变动

不法分子先窃取受害人网银账号和密码，通过购买贵金属、活期转定期等操作制造银行卡上有资金流出的假象。然后假冒客服骗取用户信任，称如需退款需要受害人提供自己收到的验证码，受害人一旦提供给对方，网银里的钱便会被全部转走。

### 五十七 补换手机卡

不法分子先用垃圾短信和骚扰电话轰炸用户手机，以此掩盖由官方客服发送的补卡业务提醒短信，然后，拿着有受害者信息的临时身份证去营业厅现场补办手机卡，使机主本人的手机卡失效，以此接收银行短信验证码，从而把银行卡的钱盗走。

### 五十八 换号了请惠存

不法分子假冒机主给手机里的联系人发短信，声称换了新号码，获得信任后进行诈骗。



扫码关注  
警事公众号

**如遇被骗及时拨打 110 报警电话，并与学校保卫处进行联系： A 区：65100110 B 区：65120110 C 区：65118110 虎溪：65678110 。更多防骗资讯，关注“平安重大”微信公众号：**

