厦门大学网络安全教育

各位同学（本文虽长，字字血泪教训，请认真看完）：

近年来，虚假信息诈骗已成为严重的社会治安问题，据公开报道，2015年中国居民被诈骗损失超过222亿元。据公安机关通报，高校学生也屡屡上当受骗，损失不少财物。据了解，绝大多数受害人已通过电视、报纸、宣传单等方式接触过防诈骗宣传，但还是存在“灾害自我例外”的侥幸心理。虽然了解一些诈骗形式，却不相信会发生在自己身上，从而对防骗宣传关注度不够、警惕性不高，最终上当受骗。目前高校里较常出现的诈骗手段高达**24种**，包括：冒充客服、网购诈骗、刷信誉度、冒充领导老师、冒充QQ好友、机票改签、冒充公检法、冒充政府工作人员、邮包涉案、网络中奖、网络兼职、网购游戏币、猜猜我是谁、QQ交友、银行卡社保卡涉案、网购机票、冒充同学亲友、借钱诈骗、诈骗链接、网络招工、借卡转账、兑换积分、网上充值、淘宝积分、电话中奖、诈骗链接等。面对花样百出的诈骗，要牢记：不听、不信、不转账、不汇款！如果遇到可疑情况，及时跟家人、朋友等商量，或者自己拨打公安机关咨询电话，避免上当受骗。

**一、主要诈骗手法介绍**

1、冒充公检法、电信等部门的工作人员或部门等的电话。以事主电话欠费，查收法院传票、包裹单等借口诱骗事主回电咨询，然后以事主个人信息泄露，银行账户涉嫌洗钱、毒品犯罪或需要调查等为由，要求事主将银行存款转至对方提供的所谓“安全账户”审查，从而实施诈骗。

 　2、“猜猜我是谁”。冒充领导、老师、同学、亲戚朋友，以借款名义诈骗。不法分子冒充受害人的熟人，在电话中让受害人猜猜他是谁，当受害人报出一熟人姓名后即予承认，先是寒暄联络情感，不日，再打电话编造因赌博、出车祸、生病等各种事由急需用钱，向受害人借钱并告知汇款帐户。

3、冒充税务部门退税诈骗。通过非法手段先获取事主资料，然后通过固定电话、手机或者短信冒充车管所、税务机关工作人员，以“办理汽车、摩托车、农用车购置税或者教育退费”为名诈骗。

4、冒充银行工作人员和银行客服短信提醒，以“事主银行卡扣除年费或在外地巨额消费、透支”等为由诱骗回电咨询，然后以事主银行卡信息泄露需要开设安全账户服务实施诈骗。

 5、“引诱汇款”诈骗。不法分子以群发短信的方式，将“请把钱或房租存到XX银行，账号XXX，王先生”等短信内容大量发出。有的事主碰巧正打算汇款，收到此类汇款诈骗信息后，即可能未经仔细核实，将钱直接汇到不法分子提供的银行账号上。还有的事主因拖欠别人钱款，收到此类诈骗信息时，自认为是催款的，没有落实真实姓名，便匆匆把钱汇入该银行账号。

6、虚假中奖诈骗。方式主要分三种：①预先大批量印刷精美的虚假中奖刮刮卡，通过信件邮寄或雇人投递发送；②通过手机短信发送；③通过互联网发送。受害人一旦与犯罪分子联系兑奖，即以“需先汇个人所得税”、“公证费”、“转账手续费”等各种理由要求受害人汇钱，达到诈骗目的。

7、假装 QQ亲友借款诈骗。不法分子事先通过盗号软件和强制视频软件盗取QQ号码使用人的密码，并录制对方的视频影像，随后登录盗取的QQ号码与其好友聊天，将录制的视频播放给其好友观看，以骗其信任，最后以急需用钱为名向其好友借钱，从而诈骗钱款。

8、医保卡信息诈骗。不法分子利用改号软件冒充医保部门工作人员，谎称事主的医保卡有异常或刷卡记录，并将电话转接到所谓的主管部门或执法机关处理，要求事主将存款存入所谓的“安全帐户”实施诈骗。

9、手机链接诈骗。此类诈骗大多是由一条带有钓鱼网址的伪基站短信开始，如果用户打开了短信中的链接并按网页提示进行操作，会导致手机感染木马病毒，窃取个人网络支付账号密码信息，随后骗子通过网络支付工具发起款项支付，再拦截窃取所需的短信支付验证码，利用网络支付漏洞使用被害人的银行卡完成盗刷。

10、网络购物诈骗。不法分子仿制一些大型购物网站或使用插件在各大网站中发布虚假廉价商品短信（包括机票）信息，诱骗事主汇款后骗取钱财或以次充好或以假货进行诈骗。

11、冒充淘宝、京东客服诈骗。不法分子冒充客服以系统出现故障需要退款、重新支付等名义骗取对方账户、身份证、银行卡号、支付验证码等信息盗取账户资金。

12、打电话谎称受害人的亲人朋友被绑架需支付赎金或在外出事故、突发急病需住院押金。

13、网上兼职、刷信誉度进行诈骗。

**二、高校多发虚假信息诈骗案例介绍**

**1、冒充QQ好友诈骗**

诈骗分子事先通过盗号软件或强制视频软件盗取QQ号码使用人的密码，然后登录所窃QQ，冒充事主有针对性地选择其QQ好友，与其对话。骗取信任后，编造出车祸、急需周转资金等各种借口骗取钱财。部分不法分子还利用软件远程启动视频探头，事先录取事主的视频资料，在与QQ好友聊天时，向其播放事先录取的事主视频，骗取对方更大信任。

2016年3月7日18时50分许，学生姚某在散步时接到了高中同学南某某的QQ信息，请求姚某帮他的手机充值200元人民币，随后姚某通过支付宝帮其充值了200元人民币并向该同学确认，得知该同学的QQ号被盗了，遂发现被骗。

**2、网络购物诈骗**

诈骗分子在互联网发布虚假廉价商品信息，一旦事主与其联系，则要求先垫付“预付金”、“手续费”、“托运费”，以此骗得钱财。又或者制作虚假“钓鱼网站”，以低价售货为诱惑，如网上售卖低价机票等，通过在页面设置各大银行等金融机构的链接图标，当你点击时，就进入了跟上述机构一模一样的假冒网页，你的网银账号和密码即被盗取，紧接着被盗的是你的钱。其表现形式有以下几种：

⑴多次汇款。骗子以未收到货款、或提出要汇款到一定数目方能将以前款项退还等各种理由，迫使事主多次汇款。

⑵假链接、假网页。骗子为事主提供虚假链接或网页，交易往往显示不成功，让事主多次往里汇钱。

⑶拒绝安全支付法。骗子以种种理由拒绝使用网站的第三方安全支付工具，比如谎称“我自己的账户最近出现故障，不能用安全支付收款”或“不使用网易宝，因为要收手续费，可以再给你算便宜一些”，等等。

⑷收取订金骗钱法。骗子要求事主先付一定数额的订金或保证金，然后才发货。然后就会利用事主急于拿到货物的迫切心理，以种种看似合理的理由，诱使事主追加订金。

⑸约见汇款。网上购买二手车、火车票等诈骗的常见手法。骗子一方面约见事主在某地见面验车或给票，又要求事主的朋友一接到事主电话就马上汇款，骗子利用“来电任意显软件”，冒充事主给其朋友打电话让其汇款。

⑹以次充好。用假冒、劣质、低廉的山寨产品冒充名牌商品。

2016年3月3日14时许，学生刘某在宿舍上网，通过58同城上的一个QQ号购买电子产品（卡西欧自拍神器），支付定金500元。卖家随即发来快递单号和查询网站。（该单号仅能在卖家提供的网站查询到物流信息，其他网站查询不到。）3月5日上午，快递公司来电话要刘某联系卖家，只有通过卖家通知快递才能发货。于是刘某QQ联系卖家，对方让他支付余款1000元。付款成功后对方又提出他们货品没有缴税，需要再支付3000元定金，等快递送货时连同3000元定金一起送还给刘某。支付完毕后刘某没等来购买的电子产品，再次联系卖家。卖家又称快递在送货途中遇到交警查车，快递员怕被查到不敢送货。接着对方提出让刘某再交5000元定金，确保没有举报他才送货。刘某拒绝再付款，提出退货退款。卖家先是同意，可之后以各种理由拖延时间迟迟不予退款。刘某意识到被骗。

**3、一点击链接就“中毒”**

不法分子利用非法手段，获取手机号码，并群发含有木马病毒程序链接的诈骗短信，被害人一旦点击后手机就中了木马病毒。该新型木马病毒能拦截手机短信，获取事主通讯录信息，同时获取关联的银行卡账户等信息，通过拦截获取支付验证码，在网上购物消费变现或通过第三方支付平台红包转账提现。诈骗短信中的钓鱼链接存在两种主要危害：一是可能含有木马病毒，损害用户手机正常使用或导致用户手机产生资费消耗；二是通过虚假钓鱼界面获取网友银行卡、身份证、电话、验证码等个人信息，可直接盗刷事主银行卡中的存款。不法分子为让事主打开链接，有伪装成移动、电信、银行、电力公司等单位号码的，也有伪装成学校“校讯通”向你发送孩子成绩等信息的，或者伪装成熟人让你看照片等等，不但手机短信有诈骗链接，微信上也时有出现，例如“喊你投票”，发送标题吸引视频等，事主一旦点击信息中的网址，木马程序便植入手机。

2016年4月12日15时14分许，学生潘某上课时接到17196882599发来的短信“潘某您好！这是您宝贝本学期各科情况和我校评语t.cn/Rqx6eFT[班主任]”。潘某点击连接后发现手机连续接到银行提示，其工商银行卡通过快钱方式转出6笔现金，共计998元。

**4、冒充淘宝、京东等购物平台客服诈骗**

　 不法分子从相关渠道获取消费者网上购物的详细消息，拨打用户电话谎称消费者所购买的物品缺货需要退款或交易平台出现故障，交易未完成，有一笔退款需要核实等为由，向事主发送钓鱼网站、木马链接等，骗取事主的身份证号码、手机号码、银行卡号、交易密码等重要信息，并要求事主回复手机收到的6位退款验证码，凭借事主给出的信息划走其银行资金。

2016年3月7日16时49分许，学生张某在寝室接到了一个自称是淘宝书店售后的电话，对方以支付宝出了问题没收到付款为由，要求张某申请退款重拍并加其QQ以提供一个网上退款平台。该同学点击了该退款平台链接，按照对方指示操作并告诉了对方银行卡信息与验证码。但对方又告诉他操作不成功，需向别的同学借银行卡操作，于是张某先后借宿舍两名同学的两张银卡，按照对方要求操作，结果三张卡被骗转11904元。

**5、兼职刷信誉诈骗**

不法分子事先制作好了相应的网页，看上去极像正规的商铺，上面的商品也是普通商品，但点击进去却会链接到别的地方，多是Q币或游戏币、充值卡等即时到账的商品。事主一旦确认购买，就等于为他们预先设定的用户充值了。在“网上代刷兼职”的骗局中，上当的大多是年轻人。通常的诈骗手法是在前几次的操作中，对方会让事主先刷小额的交易，有时也会退款，取得信任后再让受害人刷大额的物品进行诈骗。

2016年5月13日19时，学生曾某在宿舍手机上网，在赶集网投简历找兼职。曾某发现一家自称正规公司，专门帮各大商城做销售量的兼职信息，于是加了对方QQ进行联系。对方要去曾某的个人信息后称核对后就给安排任务。之后对方安排曾某为中国电信公司刷销量。他们发给曾某一个网址，要求曾某点击购买网页上面值500元的11888充值卡，并让曾某填写商家验证手机号码18049743860。曾某疑问是否是给对方充话费，对方矢口否认，称交易结束后会连同报酬一同返还。最终曾某还是用支付宝分9次购买了该充值卡，共计支付4500元。但支付后对方以系统故障，本人操作失误等理由推脱迟迟不见资金返还。

**6、冒充领导、老师诈骗**

当你接通对方来电并询问是何人时，不法分子故弄玄虚先让你猜猜他是谁，如果你猜想是某某人时，对方便顺势称你猜中，之后以各种理由借款。类似冒充领导、老师、同学、亲戚、好友，以借款名义进行诈骗的，均属于“猜猜我是谁”诈骗类型。

2016年2月24日17许，学生左某接到一个电话，对方以“你知道我是谁吗？”让左某猜。左某听声音感觉是“朱老师”就回答说是“朱老师”，对方自称是，并让左某第二天9点到老师办公室。第二天左某去老师办公室的路上接到对方来电，对方称领导找他这下不在办公室，又因为急需用钱，向左某提出借款要求。左某按对方要求转账1000元到指定帐号。转账后再联系对方来电号码，提示为空号。之后左某与真正的朱老师联系上，询问此事时得知自己被骗。

**三、防诈骗提醒**

**1.** 对于短信、QQ、微信等收到的不明推送链接，都很可能是诈骗网站的链接，切勿随意打开！！尤其是手机里装有支付宝、微信支付或网上银行的，所绑定的银行卡内存款很容易被窃取。

**2.** 在转帐之前可先电话联系收款方（必须使用原来保留的电话号码，或者官方途径获得的电话号码，不能使用对方的来电号码，切记！），再次确认后再转。

**3.** 若发觉自己被骗，立即采取自救措施！

骗子得手后，一般不会亲自去ATM取款或转账，而是通过网上银行将账款转给各个取钱小弟，由他们分散取出后汇总。所以，发觉被骗后，立即采取自救措施，通过连续多次输错密码的方式，锁定骗子的网银账号，有可能可以阻止骗子转移资金。

第一种方法：拨打诈骗账号归属银行的客服电话——根据语音提示输入诈骗账号——重复多次输入错误密码

第二种方法：打开诈骗账号归属银行的官方网站——在网银登录页面输入诈骗账号——重复多次输入错误密码

采取自救措施之后，再立即报警！

如有疑问，可免费拨打福建警方防诈骗咨询热线：96110-8

保卫处24小时值班电话：2188110

大学路派出所报警电话：110、2510110

厦门大学保卫部（处）