

安徽建筑大学保卫处

校园警讯

(2021年第3期)

保卫处报警电话：北区 0551-63513112；南区 0551-63828112

警惕!电信诈骗真实案例，就发生在身边

各二级学院、相关部门：

据公安部门通报，今年以来，网络电信诈骗案件频发，尤其是在校大学生属案件高发群体，给大学生造成巨大的财产损失，现将近期发生的大学生网络电信诈骗案进行通报分析，警示全校同学提高警惕，引以为戒，防止上当受骗。

一、案例回顾

1、【案例实录——兼职刷单诈骗】

案情回顾：张同学于2021年10月18日14时在淘宝网上找兼职并购买了一个平面设计兼职单，之后诈骗分子让其加了一个微信号，之后这个微信号就让学生通过链接下载“优信”APP，注册之后在APP内就有助理加其为好友并拉入一个任务群，群里面都是发布关注微信公众号的任务，张同学也跟着后面做了几单，就是普通的微信关注任务，每单完成后对方都通过微信收款码返现3元，后来群里面又发布新的“预存返现”订单（就是联系助理后，对方给学生提供一个银行卡账号和姓名，再通过自己的网银往里面转账后返

本金和佣金到 APP 余额，受害者再通过余额提现到自己的银行卡上的任务）。学生第一笔转账充值 300 元，获得 220 元的“收益”，接着从余额内成功提现 520 元到自己的银行卡内，第二笔开始转账充值了 500 元，结果诈骗分子说必须做满连单任务才能返现，后面又分别转账 1588 元、4588 元、4300 元、25888 元、30000 元、58888 元、188888 元、150000 元，一共被骗 464420 元。



案例分析：网络刷单类诈骗常以“返利”为诱饵，引导“刷单员”不断的对其账户充值转账，并在约定时间内向“刷单员”连本带利返还一定的金额，直到骗取更大金额后借故不再返款。虽然该生已下载国家反诈 APP，并已按照要求打开软件、来电、短信等拦截提醒功能。但由于学生警惕性低、贪心心理、诈骗分子利用新软件实施诈骗等原因，导致学生仍然被骗。

2、【案例实录——冒充好友诈骗】

案情回顾：张同学在 2021 年 11 月 11 日傍晚 18 时，不法分子冒充该同学的弟弟用 QQ 给该生发消息，该同学当时并不知情，也没有进行怀疑，对方称朋友在医院看病，缺钱，

向该生借了三千元，该同学将钱用支付宝口令红包转给他以后，忽然想起辅导员开班会时说的遇到钱款网上支付时，一定要电话核实，可惜想起来时已经晚了，经过核实后该同学发现被骗了，于是立即报警。



案例分析：此类诈骗迷惑性最强，骗子首先利用网络漏洞盗取 QQ，利用 QQ 自带好友备注，确定受害人与被盗 QQ 的可能关系，然后向受害人发送信息。冒充 QQ 使用人，以同学生病，自己急需用钱等理由，诱使受害人对其进行转账汇款。请同学们记住，防范电信诈骗，请做到不轻信、不透露、不转帐，遇到 QQ、微信好友跟你借钱时，一定要核实身份。

3、【案例实录——网络赌博诈骗】

案情回顾：2021 年 10 月 26 日晚 19 点左右，张同学因心情烦闷，在一个学生自发建立用于日常交流的 QQ 群里，看到有人发寻找聊天的人，于是就加为好友，对方直接发了一个链接，学生下载注册了 APP，打开以后，就有人联系提供下注信息，并发了一个银行账号用于转账。学生按提示充了 500 余元，APP 账面显示有金额，按提示下注后，账面显示有收益，于是就希望提现结束，但是被告知不能提现，要

求必须下注三次才能一起提现。为了追回金额，在骗子的一步步引导下，学生分三次进行了转账，第一次 500 余元，第二次 2500 余元，第三次 10000 余元，共计三次 13000 余元。之后学生要求提现，但是对方说不能提现，要求继续下注，但是张同学没有钱了，对方说“没有办法了，放弃吧”，学生遂发现上当受骗了，于是到锦绣派出所报警。



案例分析：骗子先是以网友结识，通过一阶段聊天取得信任之后骗子就会说在某个博彩平台上赚钱了诱导网友跟其一起玩，大多数人刚开始抱着玩玩的心态但是一旦尝到甜头之后就大量的下注，接下来就会被骗的血本无归。时刻谨记，网络赌博绝非正途，十赌十输，不要听信谣言、不要相信一夜暴富，不要去拿命运赌博，因为你面对的不是命运，而是一场精心设计的骗局。网络赌博，你只要接触了，不是犯罪就是倾家荡产。

4、【案例实录——“双十一”退款诈骗】

案情回顾：11 日下午 5 时许，张同学收到一条短信——

“尊敬的买家，临时发现库存的衣服存在瑕疵，为保障您的权益，我们将取消订单，烦请点击以下网址，办理退款手续。”衣服没买成，多少有点郁闷，不过张同学被卖家周到的服务和诚恳的态度打动，立即点击短信里的网址准备接收退款。然而打开网页后，发现退款并不是走的“支付宝”流程。淘宝购物最有力的保障就是支付宝，不走支付宝退款，心里总不放心。张同学于是发短信咨询卖家。对方回答得似乎合情合理：“淘宝有规定，退款会影响好评，这批货退款太多可能会被封店。”张同学体谅“卖家”的不容易，按照短信里给的网址，在上面一步步进行操作，卡壳的地方则通过电话和短信交流，半小时就完成了“退款手续”。然而，当张同学晚上查看银行卡时，却发现根本就没有收到什么退款，甚至卡里原有的 10980 元现金也在下午被转走，发现被骗，随即报警。



案例分析：“双十一”过后，不法分子常以“退货”或“退款”为由假扮客服，要求消费者点击其提供的“钓鱼网站”链接，盗取持卡人的银行卡密码及动态验证码。谨慎对自称网络客服的电话或短信，切莫泄露银行卡账号、户名、动态验证码等信息。

5、【案例实录——冒充客服付款卡单诈骗】

案情回顾：11月12日上午9时许，张同学突然接到一个所谓“支付宝客服”的电话。对方称，张同学11日一笔交易在付款过程中出现了故障，无法显示已付款，因此不能发货。因为“双十一”期间“秒杀”的货物数量有限，张同学急忙向“客服”寻求解决办法。很快，这位“客服”加了张同学的QQ，并在QQ上发给该同学一个链接网址，称按照这个网站的要求操作就行了。张同学打开这个显示为“淘宝网异常订单处理中心”的网站，果然看到自己的订单确实“失效”了，便信以为真。接下来，张同学按照“客服”说的一步操作，重新填写了自己的支付宝信息、密码。一会儿后，该网站显示张同学订单生效了。原以为事情就此解决，但随即手机上的一条短信让张同学一下子懵了，短信显示自己的支付宝被扣了1000多元。张同学急忙拨打“客服”的电话联系，“客服”表示这是虚拟信息，钱会返还，但需要提供动态密码。张同学再次按“客服”所说的步骤操作了一遍。就这样，多次操作之后，张同学卡上的钱被扣了51000元。当张同学再与刚才的“客服”联系时，却发现这个电话已经打不通了。这时，张同学才意识到自己遇到了网络诈骗。



案例分析：由于“双十一”期间网购订单太多，丢失、退货退款此类信息容易让人信以为真。其实，所谓的“卡单”、“掉单”、“交易异常”、“解冻订单”、“异常订单处理”等词汇全部都是诈骗专用术语，淘宝、京东等正规电商的网络交易平台上不会出现这些词汇。如果遇到交易异常或发货缓慢的情况，一定要拨打电商网站的官方客服电话进行咨询，切勿相信陌生人打来的电话或发来的短信，更不要轻易点开陌生人发来的网址链接。

二、防骗技能

1. 加强防范，保护好个人信息，无论何时何地都不要轻易透露自己的身份证号、银行卡号、密码、手机验证码等个人信息，这些信息是不法分子诈骗成功的必备条件，若能保护好任一条信息，都将提前终止不法分子的诈骗行为，防止上当受骗。

2. 对于来自 QQ、邮箱等网络平台，电话、短信、微信等电信平台另一端的陌生人的信息提高分析辨别能力，即使是熟人甚至是关系要好的亲戚朋友，都应对相关信息加以验证确认后，才可付诸行动，否则，后悔晚矣。

3. 日常生活和学习中，对一些陌生短信、QQ 等信息做到不轻信、不贪婪、不理睬，这是对付网络电信诈骗的杀招。

4. 当认为信息十分重要或事态严重，但自己又不能辨别信息的真假时，切记要在第一时间向辅导员或保卫处反映求证，切不可盲目行动。

主题词：治安、诈骗、安全教育

抄送：学生处、各学院、辅导员

印发：各班级