**下沙高教园区2016年3月通讯网络诈骗典型案例**

本学期开学以来，高教园区诈骗案件继续频发，且呈现出诈骗方式老套、诈骗金额高等特点，现挑选出部分案例进行整理分析，望广大师生学习防范，避免上当受骗。

* **以涉嫌诈骗、有洗钱等违法行为等形式诈骗。以上海嘉定警方的名义进行的诈骗有多起。**

**案例：**某同学接到电话为+8996584618的号码称其在上海办的一个号码可能涉嫌诈骗，将其转接到+99959995000的电话号码，电话那头自称是上海嘉定区的民警，称其涉嫌一个诈骗案，需要将所有的钱转到一张卡上再汇入指定的安全账户，该同学通过工商银行ATM机向对方的工商银行账户分三次汇入131505元。后发现上当受骗。

**特点：**能准确说出你的基本信息，或者用诱骗的方式让事主说出基本信息。比如以核对身份证信息为理由先让你说出身份证后四位，然后再询问你的出生年月，套出同学的身份证号码。同时在此期间不允许事主挂断电话，直至汇款上当受骗为止。

**谨记：**如果学生有违法行为，公安机关一定会通过学校相关部门联系学生，而不是用电话直接联系本人。

1. **冒充学校老师或领导骗钱。**

**案例：**某学院老师接到冒充学校院长的电话，让其买信封帮助送礼，然后以银行卡金额不足为借口，要求该老师通过支付宝转账2000元。后与院长核实发现上当受骗。

**特点：**可以准确的称呼事主的姓名，然后以院长、领导、导师等名义与事主交谈，最后以送礼、汇款等名义，委托事主汇款，一般在1000至1万之间。

**谨记：老师和领导是不会通过短信或者QQ向学生借钱的。**

1. **以淘宝刷单、找兼职、投资返利等为借口诈骗。此类诈骗案件占三月份高校学生被骗案件中的50%以上。**

**案例：**某高校学生加入某新生群，[看到群里有人发布兼职刷单信息，后其通过QQ加对方为好友，加完以后对方让其填一张申请表，并发给其一个二维码，让其通过支付宝扫描二维码的方式进行刷单，该生将2000元钱转入对方支付宝（账号mgw\*\*\*@163.com，账户名字是“深圳市创盛冠瑞科技有限公司”）内，发现被骗，损失人民币2000元。](mailto:看到群里有人发布兼职刷单信息，后其通过QQ加对方为好友，加完以后对方让其填一张申请表，并发给其一个二维码，让其通过支付宝扫描二维码的方式进行刷单，该生将2000元钱转入对方支付宝（账号mgw***@163.com，账户名字是)

**特点：**以刷单找兼职等借口，寻找新生或者需要勤工助学岗位的学生，诱骗对方刷二维码进行所谓的刷单。

**谨记：**无论是58同城、淘宝、贴吧、QQ群等地方的网络兼职刷单一律是诈骗，千万不要相信。

**四、网上交易虚拟游戏币、游戏装备等诈骗**

**案例：**某高校学生帮人购买虚拟游戏币，有一个人微信（账号VIP13394187777，名叫“王小贱”）的人加其微信，双方进行了一些交易，信誉良好。近日，对方告诉该生他有一个价值168000元的虚拟币激活码，问其是否购买，该生刚好有一个客户需要购买。于是该生跟“王小贱”联系 表示购买，后按照之前操作方式，把168000元通过网银转账的方式分三笔账到账户内，然后对方就发给其一个激活码，完成了交易。第二天客户告诉其这个激活码无法正常使用，该生联系“王小贱”称会帮其解决的，后对方将其的微信拉黑，电话删除了，其才发现被骗，损失168000元人民币。

**特点：**陌生人汇款，前期小额交易基本维持正常，慢慢开始进行大额交易。

**谨记：**不要随意给陌生人汇款。

1. **通过微博账号、微信账号、百度贴吧买卖门票、机票、火车票等。**

**案例：**某高校学生上网使用微信购买演唱会门票，通过微信绑定的银行卡向对方人民币2620元，后没有收到门票，并且微信被对方拉黑，发现被骗

**特点：**对方要求线下直接付款，然后再发货。

**谨记：**没有核实前，不要给陌生人汇款。

**六、冒用亲戚、熟人的支付宝、QQ等诈骗。**

**案例：**某高校学生手机QQ收到冒充其姐姐QQ的信息，要其联系一个航空公司的程经理，称其姐姐已经预定了两张机票，没有付钱，并给其一个中国银行卡，后其通过支付宝向对方转账10400元，后发现被骗。

**特点：**冒充亲戚、朋友的支付宝、QQ、微信等信息，用链接的方式发给事主进行付款，实现诈骗。

**谨记：**不要随意点击短信、QQ、微信中的链接地址。进行汇款前一定要核实。