

安徽建筑大学保卫处

校园警讯

(2022年第4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：

端午假期即将到来，为切实提高师生对电信诈骗的风险防范意识和应对处置能力，维护师生生命财产安全，保障校园安全稳定，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。



1. 虚假购物

2022年4月23日，杨同学向公安机关报案，称其在微博上看到有人发布关于预约HPV疫苗的信息，于是联系对方。对方声称可以帮其预约。于是，杨同学将自己的个人信息告知对方，随后，收到一条陌生号码发来的短信，称杨同学已经成功预约接种HPV疫苗。对方从微博发给杨同学一个银行账号，让其支付费用2858元，杨同学转账后，对方又以转账时没有备注钱款用途和订单被关闭为由又让杨同学转账两次(分别为2858元、2868元)，杨同学转账后，对方仍称未收到钱款，杨同学意识到自己被骗。

案例分析：网购时一定要选择正规的购物平台，切勿私下交易。对异常低价的商品请加强甄别，详细了解商家信息，确定商品真实性，不要轻易给陌生人转账或者汇款。一旦遇到“卡单、调单、激活”等关键词，请一定要提高警惕。如遇到类似情况，请及时拨打96110进行咨询求助。

2. 冒充电商物流客服诈骗

2022年5月2日，丁同学向公安机关报案，称其接到一陌生电话，对方自称是淘宝客服人员，并表示因丁同学前期在网上购买的商品质量有问题，需要对其进行理赔。由于对方准确说出了丁同学的购买商品名称及个人信息，于是丁同学并未起疑心，添加了对方提供的QQ号，并按对方要求扫描了一个二维码，填写了银行卡号码、验证码等个人信息，随后发现自己的银行卡被盗刷。

案例分析：正规退货退款，请在购买平台进行操作，款项会由支付渠道原路退回，不需要再提供银行卡号、验证码等个人信息，更不会以此为幌子要求下载各类虚假APP。一旦遇到“客服、理赔、提高信誉”等关键词，请一定要提高警惕。如遇到类似情况，请及时联系购买平台进行核实或者拨打96110进行咨询求助。。

3. “杀猪盘”诈骗

2022年5月24日，张同学向公安机关报案，称有一陌生人通过QQ音乐评论区联系张同学，并添加张同学微信好友。此后，对方一直与张同学保持网上联系，最终和张同学确定恋爱关系。在博取张同学信任后，对方以自己在工作期间使用手机不便为由，让张同学使用其账号帮助其“投资”一款期货，待张同学相信获利后，对方让张同学也一起参与投资，待张同学投入大笔金额后，便将张同学拉黑、取关，张同学才发现自己被骗。

案例分析：网络交友需谨慎，涉及金钱往来一定要提高警惕，天上不会掉馅饼，不要被所谓“低成本、高回报”迷惑，切勿相信稳赚不赔的“买卖”。投资理财应该选择正规渠道和合法机构，不要相信来历不明的网络平台和APP。

4. 刷单引流诈骗

5月11日，张同学被一陌生网友拉进QQ群聊，群主称招募刷单兼职，张同学随即点击了群内发布的链接，下载了一款名为“购物”的APP。随后，一名业务员联系张同学，称可以指导张同学进行操作，并发送一银行卡账户，让张同学向该账户转账下单。张同学完成任务后，成功提现本金及佣金。随后，对方让张同学又下载一款名为“飞驰”的APP进行投资，张同学投资前三笔小额资金后，均成功提现本金及利润。当张同学投资大笔额度后，发现账号冻结，无法提现。对方以操作失误、网络卡顿等借口让张同学转账多次，均无法提现，张同学发现自己被骗。

案例分析：刷单就是诈骗。刷单违规违法行为，国家法律法规、电商平台均明令禁止这种虚假交易。警方提醒，从传统的购物刷单到点赞、关注、刷视频等套路，本质上都是刷单诈骗，而且，不法分子的诈骗手段越来越呈现出

“混合打”模式，广大师生一定要提高警惕，不要有“贪图小便宜”“轻松赚大钱”的心理，也不要轻信所谓的高额回报，更不要轻易点击陌生链接、下载陌生 APP。

保卫处特别提醒：

1. 接到“退款”、“返钱”一类的电话不可轻信，应第一时间通过网购平台联系商家进行核实，如的确属实，务必通过网购平台正规渠道进行退款；

2. 不要随便点开陌生人发来的链接、二维码；

3. 不要随便在外来网站上填写私人信息，如银行卡账号、密码、验证码；

4. 千万不要相信退款需要通过第三方借贷平台借钱转账刷信用度；

5. 遇到诈骗，请第一时间拨打110报警。

谨记：

**未知链接不点击
陌生电话不轻信
个人信息不透露
转账汇款多核实**

请辅导员务必开班会覆盖到每位学生！

主题词：治安、诈骗、安全教育

抄送：学生处、研工部、各学院、辅导员

印发：各班级