可能存在的一些“诈骗”新生的坑

【前排提示】此处的诈骗不是法律意义上的诈骗，部分事件本质上来说算是推销，只是因为性价比较低，我们称之为“诈骗”，特此声明。

一、线下部分

1. 不得不提的校园卡推销

在新生入学前，在我们的宿舍园区就会搭起一个推销校园卡的棚子，会有不少学长学姐“像恶狼一样”盯着新入学的同学，尝试推销移动、电信的校园卡，并从中得到提成。

校园卡本身还是具有一定性价比的，相比一般套餐而言它的流量与话费都更多，同时也会送一些影视软件和音乐软件的 VIP 等等。但是浙大校园内是提供全范围覆盖的 WIFI 网络的，大家在日常学习生活中也不得不使用浙大校网来访问一些浙大内部网站，因此看似便宜的流量套餐其实是一个鸡肋，更不用提话费套餐了（和家长打电话可以用亲情网免费通话，和同学之间的交流为什么不用微信或者 QQ 的语音通话以及 Facetime 呢？）。此外，校园电话卡会**提供一个新的电话号码**，而大家的**支付宝、微信支付**以及其它相对私密的软件都是用**与原号码绑定**的，重新绑定也是一件相当困难的事情。因此，如果你已经有了自己的电话卡（不会真的有人没有吧），学长组极不推荐购买新的校园卡，真的需要杭州地区的电话卡也建议大家之后到尧坤楼的移动办事大厅办理，可以免去中间商赚取的差价。

至于如何拒绝推销办卡的学长学姐，一句**“我已经有了”**就可以解决所有问题。（不要说自己不需要，这样还是会给推销者留有余地，浪费自己的时间）

2. 卖被子的推销

部分同学可能因为家里离浙大比较远，没有办法把被子带来。对于这种情况，大家可以考虑提前 2-3 天把被子和生活用品快递到我们宿舍园区的菜鸟驿站，或者可以在浙大钉生活住宿的那个板块提前预定一套生活用品（包括被子、枕头、被套、枕套等，质量不算多高，但是能用，相当齐全）。卖被子的推销者一般会通过线上混入我们的班级群尝试进行销售，这些人会由学长组来检查、剔除，但在报道期间仍可能会有推销卖被子的同学，如果你没有自带被子也没预定，也大可不必选择推销者的被子，直接到学校开放的领取生活用品的地方购买即可（甚至可以只买一部分）。

3. 宗教、邪教宣传

（以下针对的是无宗教信仰同学，如果冒犯到有宗教信仰的同学还希望不要介意）

浙大校园内还是会碰到一些（我就碰到过两次）宣传宗教的人的，他们会给你一些传单或者小册子之类的，甚至可能会给你一些好处，邀请你帮他们发发传单。在大概扫一遍确定有关宗教、邪教或者传销内容后，不要回头直接离开就行。需要注意的是，在浙大宣传宗教是一种违纪行为，是会受到处分的（处分就会退院），大家一定要千万注意！

（最后强调一下：一些宣传自己组织社团的同学看起来可能也像传销的（bushi），但是如果大家听到或者看到“竺院学生会”“竺院团委”“竺院学促会”等 title，还是可以放心听他们来一波洗脑的）

4. 邀请手机助力

这种情况在校外比较普遍，尤其是在堕落街觅食的时候，可能会有一些人拿着便宜的小礼物（比如扇子等）让你扫一个二维码助力或者关注。这个时候千万不要贪小便宜，直接**拒绝说自己不需要就好**，因为你根本不会知道二维码的背后究竟是什么东西，或许在你扫描的瞬间你的个人信息就被盗取了。

二、线上部分

线上部分我们主要集中于电信诈骗，请牢记以下几种电信诈骗方式，并避免出现：

第一种是冒充公检法诈骗。诈骗分子冒充公检法工作人员拨打受害人电话，以受害人身份信息被盗用、涉嫌洗钱犯罪为由，要求将其资金转入所谓的“安全账户”配合调查。

防诈贴士：公检法办案会通知当事人到执法场所，出示证件、办理手续。凡是不见面、不履行相关手续就要求转账、汇款的，请一律拒绝。

第二种是医保、社保诈骗。诈骗分子冒充社保、医保中心工作人员，谎称受害人社保卡、医保卡资金出现异常，可能涉嫌犯罪，从而诱骗其将资金转入“安全账户”或其第三方支付账户后再转至指定银行账户，骗取资金。

防诈贴士：接到此类电话、短信，请首先向医保、社保等机构咨询核实。

第三种是二维码诈骗。诈骗分子以打折、团购为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒。一旦扫描安装，木马就会盗取银行卡号、密码等个人信息，然后实施盗划资金。

防诈贴士：不要随便扫描二维码，扫二维码后先辨别网址真假。如果不能辨别，请不要安装，以防被骗。

第四种是代购诈骗。诈骗分子在微信圈假冒正规微商，以优惠、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”等理由要求付款，一旦获取购货款就拉黑，无法再联系。

防诈贴士：网上购物请使用支付宝等安全付款方式。

第五种是点赞诈骗。诈骗分子冒充商家发布“点赞有奖”信息，要求参与者将姓名、电话等个人资料发至微信等平台，套取个人信息后，拨打电话声称已中奖，随后以交纳“手续费”“保证金”等形式实施诈骗。

防诈贴士：遇到此类事情，不轻信、不转账、不汇款。

第六种是刷卡消费诈骗。诈骗分子通过群发刷卡消费欺骗短信，引诱回拨短信上指定的号码查询，然后冒充银联中心或公安民警连环设套，要求受害人将银行卡中的钱转入所谓“安全账户”或套取银行卡号、密码实施盗划。

防诈贴士：遇到此类事件，请通过银行公布的客服电话或到银行网点查询，千万不能向对方透露银行卡号和密码。

第七种是退款诈骗。诈骗分子冒充淘宝等公司客服拨打电话或者发送短信，谎称受害人拍下的货品缺货，需要退款，要求购买者提供银行卡号、密码等信息，实施诈骗。

防诈贴士：遇到此类情况，请不要相信，直接向卖货商家联系核实。

第八种是钓鱼网站诈骗。诈骗分子以银行网银升级或低价抛售等理由，要求受害人登录假冒的钓鱼网站，进而获取受害人银行卡号、网银密码、交易验证码等信息实施犯罪。

防诈贴士：钓鱼网站与官网往往只有很小的差别，请认真识别比对。如果不能确定，请通过银行等企业客服电话咨询核实。

第九种是刷单诈骗。刷单是指店家付款请人假扮客户购买店家商品，承诺后续返回本金和返点。刷单一般由“买家”先垫付货款，为卖家的网店提高销量和信用度，并填写虚假好评，卖家承诺及时返还本金和返点。实际“买家”刷单后不返回本金或小额返现、大额失败，并配套其他连环套路骗取“买家”资金。

防诈贴士：刷单行为本身就是欺诈行为。刷单是幌子，骗钱才是真目的。切勿相信网络上类似“足不出户、日进斗金”“轻轻松松赚钱”的兼职广告，坚决拒绝任何需要提前垫付资金的兼职工作。

总体而言，请牢记以下电信诈骗反诈秘籍六个一律、八个凡是：

六个一律：

只要陌生人一谈到银行卡要转账，一律挂掉；只要陌生人谈到，中奖了要先交税，一律挂掉；只要一谈到“电话转接公检法”，一律挂掉；陌生短信让人点击不明网址链接，一律不点；微信不认识的人发来链接，一律不点；一提到“安全账户”，一律删掉。

八个凡是：

凡是自称“公检法”要求汇款，都是骗子；凡是叫你汇款到“安全账户”，都是骗子；凡是通知中奖，领奖要你先交钱，都是骗子；凡是通知“家属”出事要先汇款或转账，都是骗子；凡是在电话中索要银行卡信息及验证码，都是骗子；凡是让你开通网银接受检查，都是骗子；凡是自称领导，要求汇款或转账，都是骗子；凡是陌生网站，要登记银行卡信息，都是骗子。

除此之外，有很多起诈骗都是所谓熟人（可能是家人，以前的同学，甚至可能是我们新生群的群友们）被盗号然后要求提供支付宝、银行卡等信息，他们的作案手段十分高明，可能在你这一步只是将你充当它们诈骗的中介，因此即使是一些看起来无害，但是涉及金钱等的都要特别当心是诈骗案件。

当我们在校内论坛（如朵朵、CC98 等平台）上购买闲置物品要慎重，特别是购买较为贵重的物品时，尽量见面交货。我们不要点来路不明的链接、扫来路不明的二维码、下载来路不明的安装包，邮箱中经常出现有关“开学通知”、“成绩通知”、“毕业回忆”等邮件，也千万不可以点开，容易引发恶意事件（当然期中期末教务处会发一个评教的邮件，请确认非钓鱼邮件后进入链接完成评教）。