关于加强学生防范网络诈骗的通知

各学院：

由于近期频繁出现大学生网络受骗的事件，为切实提高学生的自我防范意识，保证学生财产安全，请各学院务必高度重视此项工作。现就加强学生防范网络诈骗的有关事项通知如下：

**一、要充分认识做好防范网络诈骗工作的重要性**

近期正值开学季，网络诈骗形式多样，学生成为重要的受害群体。各学院务必认清当前网络诈骗犯罪的新形式、新情况、新动态，采取多渠道的宣传教育措施，防诈骗教育做到全覆盖，力求做到人人都能“识骗、防骗、拒骗”，坚决防范抵制网络诈骗犯罪。

**二、要进一步加强预防校园网络诈骗的教育与宣传**

各学院要利用网站、微博、微信、宣传栏等多种方式，向学生进行防范知识的宣传；辅导员要组织每个班级召开防范网络诈骗主题班会，让学生谈认识、谈体会，用典型案例教育学生；要加强金融、网络安全知识宣传教育，帮助学生增强金融、网络安全防范意识和对有害信息的甄别、抵制能力；要积极引导学生树立正确消费观，纠正学生超前消费、过度消费等错误观念，教育学生不贪占小便宜、不盲从、不攀比、不炫耀。

**三、要加强在校大学生的日常管理**

各学院要加强信息摸排，及时甄别“高薪兼职”、“刷单返现”等网络信息，一旦发现有网络诈骗嫌疑，及时通知学生做好防范；辅导员、四级网格员**、**学生干部要密切关注在校学生涉及财物方面的异常行为，及时发现并解决存在问题；要关注学生的经济情况，对于家庭经济困难的学生，做好精准帮扶工作；若出现学生已被诈骗团伙蒙骗，要及时做好帮扶和教育引导工作。

**四、要加强学风建设**

各学院要围绕学风建设开展形式多样、丰富多彩的活动，净化学习环境，营造积极向上的学习氛围，引导学生把主要精力转移到学习上。

学生处将对各学院工作进展情况进行走访了解，各学院活动开展情况总结于9月29日下午5点前报学生处216室。

附件：近期校园安全事件典型案例

学生处

2020年9月15日

附件：

近期校园安全事件典型案例

类型一：花样“翻新”的校园贷诈骗

目前“校园贷”诈骗的形式主要有以下几种：

通过互联网平台向在校大学生推送贷款广告，以免抵押、低利息为诱饵诱导学生贷款，并要求缴纳贷款“手续费”“管理费”“保证金”等费用，收到学生支付款项后即将其“拉黑”不再联系。

串通“职业培训机构”举办职业指导讲座，夸大培训效果，与学生签订声称能提高综合技能的培训合同，并与贷款公司勾结，诱导学生贷款支付学费，从中诈骗学生。

更为极端的，要求学生提供隐私照片、视频、身份证和家属电话号码等作为贷款抵押和担保，一旦学生无法如期还款，便以此威胁，勒索钱财。

# 案例1：2020年6月10日，大学生小张接到某男子自称为360借条的客服人员电话，该人准确地说出了小张的个人信息包括姓名、身份证号、就读学校，称该同学有一个360借条上的学生贷的账户没有注销，会影响征信。小张按照该男子的指示添加某QQ号为好友后，对方截图告知他的征信分数低，需按照他们所述的操作汇款到指定账户，征信分数达到90分后方可注销，并称注销后会把钱退回，该同学通过360借条、分期乐借款、支付宝借呗、微信借款等多个平台将合计83200元分批汇款到了指定账户，在所有汇款完成之后，该同学发现钱并未退回才意识到上当受骗。

**案例2：**2020年5月，某大学生小张接到一个陌生电话，对方自称是“京东金融注销客服”，称“国家禁止校园贷，已申请的贷款账户需要注销”，要求她按照指示，注销自己的“校园贷账户”。她此前了解过校园贷引发的争议，也曾小心翼翼地试图躲过校园贷，但致电者听起来有一定的可信度：能明确报出她的个人信息，并警告“可能有人冒用她的信息申请过校园贷”。接下来3个小时内，她按照对方的指示，从4个互联网金融平台贷出了约11万元，转到对方给出的银行卡账户上。对方说此举是为了帮她“清空额度”。意识到受骗后，她却再也打不通对方电话。

案列3：一男子网上贷款不成，反被诈骗1万元！

蔡先生收到一条贷款短信，称信誉良好可以在“微粒贷”进行贷款。蔡先生点击链接并下载了一款名为“微粒金融”的APP。

系统显示蔡先生有4万元的贷款额度，但在提现过程中，账户被冻结。“客服”表示，需先支付贷款金额的30%作流水走账，才可以为账户解冻。蔡先生随即按要求转账1.2万元“解冻费”至对方账号。

蔡先生继续操作提现，可系统再次提醒出错。蔡先生这才恍然大悟，发觉自己上当受骗了，钱没借到，反而损失了1.2万元。

原来，蔡先生遇到的贷款平台是个冒牌软件，从名称到图标全套抄袭微粒贷，仿冒微粒贷虚假放贷、收取保证金、解冻金等坑害借款人。

案例4：虚假贷款平台骗取“解冻费”

这种骗局主要指不法分子通过搭建虚假贷款平台，以“秒审核”、“易通过”、“低息高额度”等宣传诱导消费者下载APP并申请贷款，当受害人在APP内完成信息填写、额度审批等流程后，不法分子以银行卡号填写错、信誉存在问题、存在逾期记录、申请过于频繁等理由制造麻烦，告知受害人账户被冻结，无法打款，要求受害人缴纳“解冻费”、“保证金”等。

民警温馨提示：

大学生要树立正确的消费观，要充分认识网络不良借贷存在的隐患和风险，增强金融风险防范意识；

要树立理性科学的消费观，养成艰苦朴素、勤俭节约的优秀品质，尽量不要在网络借款平台和分期购物平台贷款和购物，利息和违约金非常之高；要积极学习金融和网络安全知识，远离不良网贷行为。

**类型二：**“网络刷单”不赚钱反赔本

这种骗局主要指不法分子利用当事人有兼职赚钱的心理，谎称找当事人从事“网络刷单”业务，在刷第一单时当事人会得到小额佣金，此后刷单量和金额加大，对方用各种理由欺骗当事人，但不会再得到返还的本佣金，直至当事人意识到被骗。

**案例1：学生兼职刷单被骗。**2019年5月14日，郑州某大学学生韦某某在学校宿舍时，手机接到了一条招聘网络刷单工作的短信，其将信息中的QQ号码加为好友，表示自己想做兼职的意愿后，对方在QQ上讲述刷单流程。当韦同学刷完第一单索要佣金时，对方谎称刷满三单为一个任务，任务结束后才能返还资金并支付佣金。当韦同学刷完三单，共计使用微信支付4800元后，对方将其拉黑。

案例2：一女子刷单赚提成，却被骗了4万元！

玉泉办事处李某在家中刷抖音时，一个陌生人主动加其好友，邀请其刷单。李某加了对方微信好友，对方教其刷单操作流程。

李某在扫描对方发来的二维码后支付给对方1000元进行刷单。之后李某要求对方退款时，对方告知其需要刷出支付宝借呗里的所有额度才能全额退还。李某信以为真，给对方转了4万元后被拉黑。这时李某幡然醒悟，才意识到被骗了，可是钱已经损失。

案例3：2019年10月7日，文昌派出所接到学生小颖报警，称其在宿舍上网时，看到新浪微博上有刷单兼职任务，然后小颖就添加了对方在新浪微博上留的QQ，之后对方让小颖刷单，第一次是120元，佣金5元，小颖照做了，用QQ上绑定的银行卡扫码转账给对方，过了8分钟后收到转账125元。对方提供了第二个，要下20单，小颖说自己没有这么多的钱，对方说那就先5单一结，因为数额较大，对方让我用微信转账，转完之后小颖将自己的转账记录截图发给了对方，对方提出时间超时无法返款，让小颖做完剩下的15单。小颖说自己实在没有这么多的钱并要求退款，对方坚持称要刷完剩下的单，让小颖通过蚂蚁花呗等借贷软件去借钱来完成任务，任务超时没有完成的话会被系统清零，小颖这才意识到自己被骗。

民警温馨提示：

不要轻信网上刷单广告内容，骗子把刷单当借口，用简单的要求和丰厚的利益来吸引眼球，天下没有不劳而获的钱财；

不要轻易点击或扫取陌生人发的网页链接和二维码；

保管好网络账号的密码以及身份证、手机号等个人信息，常用杀毒软件对电脑进行杀毒；

小心假客服用专业术语和“贴心”服务来获得你的信任；

发现被骗后，应及时拨打110报警，同时要注意保留证据，如银行转账记录、通信记录、聊天记录等。

类型三：游戏中的“诈骗术”

游戏账号交易是诈骗的重灾区。一种是收了钱没账号，空手套白狼；一种是交易结束后，骗子以账号被盗为名向游戏平台提交身份信息，将账号找回。第二种情况下，用户在所买账号被骗子找回后，苦于没有原始注册资料，常常无处申诉。

游戏装备也是诈骗高发区，主要有低价充值、送道具送装备、装备中奖诈骗等陷阱。具体手段包括以低价充游戏币为诱饵，收了钱就跑路；通知玩家中点券，但要求先行缴税。此外，暗含勒索病毒的游戏外挂、辅助工具也有诈骗风险，用户下载后电脑中毒，需付费才能恢复正常。

案例1：2020年9月13日，文昌派出所接到学生小王报警，称其在\*\*\*游戏上联系玩家欲购买游戏币，对方说要通过游戏平台支付，并给了小王一个QQ号，小王加上对方的QQ号，并打开了对方提供的游戏平台链接，注册了用户名。然后小王找到了平台付款的二维码，用微信零钱扫码支付了100元，并联系客服，客服说小王的个人信息填写的不全，需要充值1080元审核身份，小王就用微信继续扫平台二维码支付了1080元，随后联系客服，客服称刚才小王填写的个人信息有误，需要再充值1080元，小王信以为真又用微信扫码支付1080元。随后小王和客服说要退款，但客服称小王的个人信息里的银行卡号有错误，需要继续充值4800解冻，小王就又一次用微信扫平台的付款二维码，支付了4800元，这时客服说还要再充值4800元，用来继续审核身份信息，小王的微信此时已经没有钱了，便联系自己的姐姐，让姐姐登上自己的平台用户名和密码。随后，小王的姐姐用她微信绑定的银行卡支付了4800元。此时小王已经总共往游戏平台汇款了11860人民币，发现事情不对，就报了警。

案例：2018年3月13日，派出所接到学生小黄报警，称其在寝室里看虎牙直播上的QQ飞车手游直播，里面的说抽奖可以包中奖的，对方说最少给他700元就可以帮小黄抽奖。小黄之前在虎牙直播上也，但不是这个主播，上一次小黄给对方转钱，对方帮小黄抽到了奖，所以这次小黄就轻信了，直接给对方微信转账700元，之后被对方删除了好友。

**类型四；以包裹丢失补偿为由实施诈骗**

**案例：**2020年5月11日，某学院学生叶某某接到一个自称是圆通网点工作人员的电话，该男子称叶某某在网络上购买的物品运送途中丢失，要双倍赔偿叶某某，需要其提供一个用于收款的支付宝账号。叶某某提供自己的账号后，对方以蚂蚁积分不足为由，要求叶某某关注借呗、快马金融等平台，在平台上申请贷款，贷款下来后转入到对方账户中，以此提高蚂蚁积分。叶某某按照对方所说的方式汇款后发现被骗，共计被骗4352元。

**类型五：网购假冒淘宝客服行骗**

案例1：2019年3月4日，白杨派出所接到学生小佳报警，称其在宿舍内接到一个电话，对方自称是淘宝“小H家实拍女装”的客服，说小佳去年5月份购买她们店里的裤子存在质量问题，店家要进行回收并退款赔偿。小佳翻了手机淘宝，确实在5月份的时候有在这家店购买过裤子，就相信对方了。然后对方让小佳填写买家信息，说之后系统会处理退款，小佳也通过了对方支付宝的好友邀请，随后对方通过支付宝发给了小佳名叫“客户服务中心系统”的链接，让小佳填写信息，填写信息需要先登录支付宝账号，小佳就输入了自己的支付宝账号和密码，之后链接内显示需要填写银行信息，姓名，身份证号码，最后一个页面为验证码，验证码是通过手机短信发送给小佳的，但是小佳输入了之后并未成功，对方说让小佳试试输入支付宝密码也许会成功，小佳没有照做。此时小佳的手机收到银行的打款提醒，短信显示小佳银行卡里汇出两笔钱，第一笔是900元人民币，第二笔是1000元人民币，小佳意识到不对，对方说这是因为小佳操作太慢，系统冻结了自己卡里的钱，并给了小佳一个微信收款二维码，让小佳赶紧汇款给对方，若不赶快操作，卡里的钱将全部被冻结，小佳此时心存疑虑，便拨打了之前自称是客服的电话，可电话怎么也接不通，这才意识到自己被骗。

案列2：2020年3月20日，白杨派出所接到学生小杨报警，称其在淘宝网一家服装店选购了一件衣服，已经付款成功，但是第二天，小杨接到一陌生电话，说是淘宝卖家，对方称由于支付宝异常、订单无效，要退款给小杨。对方将小杨买的衣服、及淘宝订单号和物流信息都截图给了小杨，小杨信以为真。然后，对方很快又打来电话称正在为小杨办理退款，等会儿系统会给小杨发一条退款转账验证码，需要小杨将验证码发回。小杨发过去验证码后，自己的手机接到短信提醒，显示消费4000元，小杨意识到自己已经被骗，选择报警求助。

民警温馨提示：

在网上购物时，千万不能将银行卡号、身份证信息、手机收到的在线支付短信验证码提供给陌生人，也不要打开对方传来的网址链接，不要轻信陌生的来电或短信，不要轻易转账汇款；

在网络购物中如果发生交易失败现象，可以登录官方购物网站客服电话咨询，不要轻信百度等搜索引擎搜索到的客服电话，发现可疑情况可拨打110报警。

类型六：冒充“熟人”来骗钱

诈骗犯罪分子通过非法渠道获取公民个人信息或随机选择，通过电话、网络和短信方式，编造虚假信息，称自己是对方好友、同学甚至亲戚等熟人设置骗局，谎称有十分要紧的事情需要用钱来应急，诱使被害人汇款、转账。

案例1：2019年3月3日，文昌派出所接到学生小宋报警，称其在寝室收到同班同学QQ的消息，说帮她的手机充300元话费，小宋知道那位同学周末人不在学校，她手机可能停机就帮她充了，后来她和小宋发消息称手机还是停机，叫小宋再充500元话费，小宋没有丝毫怀疑就充了，紧接着她又让小宋往另一个手机里充值200元话费，却听到室友说也收到了那位同班同学让大家帮忙充话费的事情，小宋这才意识到自己被骗。

案例2：2018年3月16日，文昌派出所接到学生小周报警，称其初中同学用QQ联系小周，说有个朋友因为意外受伤而住院，急需用钱，让小周把自己的银行卡号发给对方，对方会往自己的卡里转1000元，然后小周再给受伤住院的朋友微信转1000元，小周想也没想就同意了，把自己的银行卡号发了过去，这时对方就发了一张汇款1000元的截图，但此时小周手机并未收到汇款提示，对方说银行的短信提示会需要一点时间，不会马上就有的，小周也相信了，就在微信上向受伤住院的朋友转账1000元。就在此时小周收到之前的初中同学的群发消息，称自己QQ号码被盗，让大家都不要相信所发的消息，小周这才意识到被骗。

民警温馨提示：

无论是QQ、微信、微博等聊天工具还是手机短信收到好友或是亲友等“熟人”发来要求转账等消息时，一定要通过拨打对方电话进行核实，如对方称电话已换号或停机，应联系其亲朋进行核实；

在聊天中如涉及汇款，一定要谨慎，以防钱财两空。

**类型七：补助、救助、助学金名义实施诈骗**

**案例：**2019年张某某通过非法渠道,事先获取了2019级新生小玉详细资料,张某冒充教育局财政局工作人员,知道小玉有资助需求，便向该生打电话、发短信,谎称小玉预留银行卡有问题,要求小玉将卡内余额存到对方提供的账户,小玉信以为真，按照犯罪分子的提示将资金转入指定账户，共计被骗9000元。

类型八：网上“养猫”还能赚钱？新型网络诈骗套路出现了

案例：十多天时间她们在网上“养猫”被骗十多万元

记者采访到了被骗的小芳和小敏(化名)。据小芳说，今年7月初，她在网上的贴吧里看到一条广告，其宣称一款名叫“喵喵”的APP，在网上养猫就能赚钱，而且还是高额回报，添加微信就能了解详情。但让她没想到的是，从她添加对方微信后，就已经步入对方的陷阱。

“我看到贴吧里有好多人都说能赚钱，就忍不住加了对方的微信，进入一个微信群里。”小芳说，刚开始，她是半信半疑，一直在微信群里观察，但连续多日看到别人转发赚钱的截图以及信息后，她就忍不住了。在7月31日，她和小敏开始往“喵喵”APP里投钱。

然而，在8月12日，“喵喵”APP突然出现问题，系统无法登录，此时她和小敏已分别往里投入了四万多元和两万多元，且一分钱的回报也没有见到。微信群里给出的解释是要更换服务器，如果想要提现之前投入的钱，就必须要继续投入，让数据能对接上，才能提现。

小芳说，当时，她们也有些心慌，不知道投入的钱还能不能要回来，可她们的群主，也是她们上线主管，表示“喵喵”APP没有问题，可以继续投钱。于是她和小敏又分别投入了两万多元。至此，她们共投入了十多万元。然而，在8月16日，“喵喵”APP就彻底登不上了。

在两人提供的转账记录上，记者看到，短短十多天，两人分别转账有十多笔，其中少的有八九百元，多的三五千元。转账收款方多为餐饮美食、服装美容、转账充值等服务。小敏说，因为她看到钱都是转给个人，不是集中在APP平台上，觉得会安全些，所以才往里投钱。“这些钱有的是我们辛苦工作存下的，还有的是家里给的。”

被骗人数有6000多人 多人不知打出去的钱是干嘛用的

小芳说，在发现“喵喵”APP和网站登不上后，各级的老板也联系不上了，群里都在传老板们卷着钱跑路了，这时她们才知道被骗。而且全国多地都有人被骗，仅他们微信群统计的就有1900多人，加上没有统计的有6000多人。

在小芳提供的一份统计名单上，记者看到，仅在8月18日晚上7时24分，统计名单中被骗人员就有1923人，被骗金额少的有两三千元，多的有十多万元，其中大多数为几万元，仅该名单中的被骗金额就多达几亿元。

采访中，记者向小芳她们询问，你们既然往里边投钱，那你们知不知道投进去的钱是干嘛用的？还有网上养猫究竟是何意？而小芳她们的回答，却让记者哭笑不得。

小芳说，她只是按操作，先在“喵喵”APP或网站上预约，然后等第二天预约成功后，后台就会发给她一个转账链接，她只需要把钱转过去，等上几天时间，钱就会被打回来，并带有最少10%的回报。网上养猫，她只知道后台在每笔交易中要求购买虚拟猫粮，其他的就不知道了。

小敏说，她理解的是，自己用钱在“喵喵”APP上预约购买一只虚拟猫，然后通过几天饲养让身价增长，等别人将其买走后，她就拿回了本金和利息。至于猫的身价是如何增长，她也不知道。

此外，记者还采访了多位被骗人，有不少人至今还不知道自己打出去的钱是干嘛用的，也不知道网上养猫究竟是何意！其中，还有人为了高额回报，是刷信用卡投的钱，目前已面临无法还款的局面。

类型九：出卖个人信息也会坐牢

案例1：近日，警方在侦办一起电信网络诈骗案是发现，涉案实名电话卡的持有人与贩卡人均为正在某高校读大一的学生梁某。一天，梁某收到一条短信“收手机卡，一张200元”，梁某用自己的身份证在网点办理了手机卡5张，提供给诈骗分子，盈利1000元。骗子利用其中一张手机卡对某公司出纳实施诈骗，诈骗金额高达87万元。警方以涉嫌帮助信息网络犯罪活动罪，将学生梁某刑事拘留。学校对其作出开除学籍处理。

案例2：2020年5月10日，商水县公安局成功打掉一个组织商水县实验中学在校学生到联通、移动营业网点开办手机卡贩卖卡团伙，抓获犯罪嫌疑人1人。2020年5月7日，犯罪嫌疑人刘某陆续组织商水县实验中学30余名在校学生到商水县联通、移动营业厅开办手机卡，每人办五张手机卡，在校学生每张获利30元，这些手机卡被转卖用于刷单诈骗。

案例3：2020年6月30日，城北分局成功打掉一个我市某高中学生出租本人微信用于兼职刷单诈骗犯罪团伙。初步查证有9名学生出租本人微信，租赁时间为白天，租金为40-50元，每日下午18时左右归还微信并付租金。这些微信号在被租赁期间，在各个社会群、同学群、亲友群和好友间群发刷单广告，以此来传播和吸引人流，实施网络代刷单诈骗。据了解，这些参与微信号租赁的学生大多都是通过朋友介绍，同学以每天有偿租赁为诱饵，吸引同学自愿租赁其微信号。形成了一个半日制租赁微信号的群体。

周口市公安局提醒：出卖、出售、出租、转借个人银行卡用于电信网络诈骗犯罪流转资金的均属于违法行为，构成帮助信息网络犯罪活动罪。中国人民银行银发【2019】85号文件精神，中国人民银行、公安部联合下发《中国人民银行 公安部对买卖银行卡或账户的个人实施惩戒的通知》银发【2019】304号文件，依法对出租、出借、出售、购买银行卡或账户的个人实施5年内暂停其银行账户非柜面业务、支付账户所有业务，并不得为其新开立账户的惩戒措施。

校园安全教育

宿舍内乱拉电线或使用违章电器致死

**案例1：**2019年，某高校学生刘某私自在宿舍内另拉电线且使用自备的插座，随着时间推移，电线的外层绝缘材料由于长期和床头接触被床头的经常晃动磨破，而该同学并没有发现该安全隐患，有一天在床上休息时被电击致死。

**案例2：**2019年9月10日，贵州黔南师院学生寝室起火，消防人员及时赶到现场灭火，在转移学生扑灭大火后，现场勘测可知学生宿舍起火原因是寝室内成员使用违规电器电热毯导致床上用品与窗帘燃烧。