

致全校教职工预防电信网络诈骗的一封信

各位教职工：

当前，电信网络诈骗案件高发，各种诈骗方式层出不穷，为了您的财产安全，请仔细阅读此信，谨防上当受骗。

一、主动联系+高收益/无风险+虚假投资=诈骗

诈骗分子通过电话、短信、QQ、微信等社交平台，以“投资老师”身份物色接触受害人，并以高收益、无风险为噱头，诱导受害人前往虚假投资APP或网站进行投资理财或外汇交易。

案例：一位陌生人主动添加了黄某微信，聊天过程中，对方声称自己在网上做理财投资可以稳赚不赔，并邀请黄某进入某投资公司微信群，群里声称有保险公司做财保，不需要担心风险，黄某抱着试试的心理，通过扫描群里分享的二维码进入投资平台，平台上显示着琳琅满目投资项目，黄某投资了几千元，得到返利后，更加大胆地去投资，平台上的返现金额越来越多，直到提现时才发现该平台已经关闭，无法进入，黄某陆续投入了13笔，共损失近30余万元。

二、网恋交友+获取信任+投资/博彩=诈骗

诈骗分子伪装成为成功人士，通过婚恋网站、网络社交工具物色诈骗对象，然后以谈恋爱名义获取信任，诱导受害人进入博彩网站、赌博APP、虚假网站进行投资理财实施诈骗。

案例：李女士在某社交APP上认识了某张姓男子，一段时间后张某向李女士宣传一个理财APP，并且让李女士帮他在上面操作管理账户，李女士操作一段时间后发现该APP能赚很多钱，遂在对方花言巧语诱惑下，李女士也开始用自己的钱充值，一开始李女士确实赚钱并成功提

现了，但在前后投入了五十多万后，再也无法联系上张某，而且投资的APP也打不开，这才发现自己被骗了。

三、做任务+小额返利+加大投入=诈骗

网络兼职刷单，刚开始做小额任务时，骗子会兑现返现承诺，让你尝到甜头，然后诱导你加大刷单本金投入，多次刷单后骗子就会以各种借口拒绝返利还本。

案例：叶女士在看到刷单的兼职广告，联系“客服”并下载APP接单，跟着导师一起做任务。叶女士按照对方指示试着刷了几单，果然赚到了一点零花钱，紧接着又投了1000元，可当叶女士提现时，却显示操作错误，需再转入5880元才能提现，急于提现的叶女士没多想便将钱转给了对方，等到的回复却是需再做一个19852元提现单才可以提现，叶女士这才意识到被骗，遂报警。

四、你犯事了+来电转接+安全账户=诈骗

诈骗分子通过非法渠道获取你的个人身份等信息，冒充公检法工作人员拨打电话，谎称你名下银行账户、电话卡、社保卡、医保卡等被冒用，或者涉嫌洗钱、非法出入境、快递包裹藏毒等违法犯罪，对你进行威逼、恐吓并要求你将资金转入“安全账户”配合调查或接受监管，进而实施诈骗。

案例：陈女士接到自称是某办案民警的电话，告知其因涉嫌贩卖新冠疫苗被立案侦查，要求其至广东某派出所配合调查，陈女士因事无法前往。随后，对方将电话转接到了广东警方。转接后，一名男子冒充办案民警，让陈女士添加其为QQ好友并发起QQ视频与陈女士聊天，陈女士见男子身穿蓝色警服，便没有怀疑，于是，陈女士按对方的要求提现到对方银行卡后，一直未收到返还，被骗金额2.3万元。

五、冒充领导或熟人+嘘寒问暖+（着急用钱）=诈骗

诈骗分子将聊天软件头像伪装成学校领导或熟人的照片，添加受害人好友后，通过假装关心骗取信任，伺机再以需要资金周转、急需用钱、签订合同等借口，要求对方转账实施诈骗。

案例：工作于宁夏某高校的董某，一天晚上，收到一陌生人加微信好友，自称是该学校新来的副校长，并让董某在第二天9点到其办公室。第二天一早，“副校长”又告诉董某，先不用来了，称有领导在办公室检查，急需用钱“打点”领导，让董某借其30万元，董某信以为真，直接给对方提供的两个银行卡号转账30万元。

六、裸聊诱惑+安装软件+录制视频=诈骗

诈骗分子先是利用“裸聊”为诱饵引诱受害人“入套”，发送暗藏木马病毒的App，窃取受害人通讯录等个人隐私信息，录制裸聊视频实施敲诈。

案例：一男子看见微信上有“美女”请求添加好友，于是不假思索地就添加了。才聊了不一会，对方先发了一个二维码让其帮扫码关注，之后又邀请其下载软件视频裸聊。视频聊天刚进行一两分钟，“美女”便发来其裸聊视频及通讯录截图，向其敲诈索要10000元，否则就将视频进行公布。该男子被敲诈10000元后，对方继续索要钱财，最后选择报警。

七、防骗安全提示

诈骗手法千变万化，但万变不离其宗，最后都是要钱或转账，所以千万不要轻信陌生人，不点击未知链接，不轻信陌生来电，不透露个人信息，转账汇款多核实。

96110是全国反诈专线，这个电话一定要接，被骗后第一时间拨打96110止损。请各位教职工下载安装“国家反诈中心”

APP，且把“来电预警”模块打开，联系手机运营商开通“骚扰电话拦截服务”功能。

最后，希望您将此信内容转告您的家人、亲友和学生，不让犯罪分子有机可乘。让我们携手共同努力，全民反诈，创建无诈校园！

南京工业大学保卫处

2022年6月17日