

投教课程讲义

一、主题：疫情下的反诈骗专题

二、课程时间：40-60 分钟

三、课程目标：分享当前社会深受疫情影响下的真实诈骗案例，总结出各种诈骗特征和防范方法，避免更多社会公众人群上当受骗。

四、课程内容

（一）讲述虚拟人物“小明”在疫情期间所遭受的各种骗局

讲个段子：朋友小明去找大师算卦，大师说他这几年会为情所困，他以为是爱情，没想到是疫情，一困就是三年，不仅仅为情所困，还为情所伤...接下来将为大家讲述我朋友小明这些年为“情”所伤的故事。

1、快速核酸检测结果诈骗

我朋友小明所在城市突然发生新冠疫情，小明原本预定了晚上出发的火车出差，根据最新防疫要求，必须持 24 小时核酸阴性证明才能出行，就在此时八卦群里出现“快速出核酸检测结果”、“加急最快半个小时”、“家里也能做核酸检测”的信息，撩动着小明的心，赶紧加好友详聊，一问得知 200 元，最快半小时出结果，直接到火车站正门取结果，只需要提供身份证电子版即可，小明一听这是解了燃眉之急啊，立即微信转账 200 元给对方，坐等核酸检测结果。约定的时间到了，小明给对方发了条微信，“消息已发生，但被对方拒收了”，然后就没有然后了...

2、虚假防疫短信诈骗

朋友小明只好重新去正规机构做核酸检测，第二天持有 24 小时核酸检测阴性证明搭乘火车出差，出差回来后突然收到一条防疫提醒，XXX 新冠肺炎疫情防控指挥部办公室提醒您：您曾在新冠肺炎确诊病例或无症状感染者活动的重点场所停留，请尽快前往就近卫生服务机构进行 7 天 3 次核酸检测，感谢您的支持配合！点击链接：<http://...完成核酸检测反馈。>

小明做完核酸后点击短信链接，进入反馈界面，显示要上传身份信息，下一步输入银行卡号、验证密码，一顿操作猛如虎，滴滴滴，某某银行短信提醒，您已成功支付 9980 元...

3、代购生活、防疫物资诈骗

随着新冠病例不断增加，防控升级，小明家里的生活物资、防疫物资大量消耗，业主群里出现了代购人员，发布生活、防疫物资售卖信息，个别自称业主的人员还声称通过代购人员真实购买到了物质。小明心想有人购买了，应该不会错，加了代购人员微信，对方要求提前支付，并约定一周后到货，小明一共支付了 980 元，购买生活用品、口罩等防疫物质。

到了约定时间，业主群里滴滴滴的信息不断，小明一看，大家都在反馈代购人员不见了，微信也找不到了，小明赶紧打开微信准备私聊代购，结果显示“消息已发生，但被对方拒收了”，然后就没有然后了...

4、虚假售卖特效药

小明这几天有点不舒服，被骗了这么多钱，着急上火，出现了感冒发烧症状，虽然核酸检测是阴性，但小明还是有点不放心，到处浏览网页，查找新冠治疗方法，突然跳出一个新冠特效药的页面，小明点击一看，提示加客服微信聊天。客服声称，公司是国有企业，有政府背景，现在出了一款特效药，不要 9800，不要 980，只需要 688，一劳永逸，永久产生抗体，小明一想，价格还不错啊，试试还是可以的，于是下单购买，等待收货，到货后一看，荷花牌清热解毒颗粒...

屡次被骗的小明，终于醒悟了，他决定痛定思痛，与骗子做斗争，通过网上不断查找资料，发现骗子们一再升级骗术，更新套路，让小伙伴们防不胜防，小明不想任骗子横行，于是绞尽脑汁，把骗子们有关疫情诈骗的新花样都整理好，熬夜整理出了一份“防诈骗指南”，

总结了疫情期间常见的“八大骗局”！

（二）疫情期间常见八大骗局

骗局一：代购物资类诈骗

骗子利用疫情期间市民买菜及购买生活物资的需求，利用微信群、网站链接及小程序等发布代购物资的信息，冒充厂家员工诱导图便宜或急需物资的市民，进行诈骗，以“要交税”、“要付押金”等理由，避开正规第三方支付平台，要求当事人通过微信私下转账、扫码交易。还会编造收取运费、收取定金优先发货等理由，诱骗当事人继续转账汇款，一旦当事人付款成功便立即拉黑。

风险提示：建议通过官方渠道订购生活物资，切勿轻信添加、下载或点击来历不明微信群、小程序和不明链接等方式，并且在购置物品交纳货款之前一定要核实对方身份。

骗局二：冒充疫苗普查调查员类诈骗

骗子通过号商批量购买账号，伪装成“疫苗接种普查调查员”或“回访员”，以社区工作人员的名义添加好友，再将当事人拉群。群内发布刷单、赌博等违法违规信息，通过一单多任务拒返佣金、流水不足无法提现等套路诈骗钱财。

风险提示：刷单是违法行为，网赌十赌十输，需提高警惕，勿心存侥幸。骗子多通过手机号码添加好友，一定要注意保护个人信息，谨慎使用添加陌生好友和加入陌生群聊。

骗局三：冒充疫情防控公职人员类诈骗

骗子伪装成“疫情防控中心”或“卫健委”工作人员，以各种理由给当事人扣上“涉嫌散播疫情谣言”的帽子，要求前往公安机关核查。攻破当事人心理防线后，主动提出将电话转接至“公安局”，以“资金清查”为由诱导当事人转账，诈骗钱财。

风险提示：公安机关不会与涉案人员有金钱往来，以涉拐/经济犯罪/非法提取社保/阻碍疫情防控等理由，要求清查资金的都是诈骗，务必警惕。

骗局四：冒充疾控中心流调人员实施诈骗

骗子冒充防疫中心工作人员，以受害者是“确诊病例密切接触者”、“健康码异常”、“核酸结果异常”需要收集受害人个人信息、行程信息为由，向当事人发送钓鱼短信，要求当事人进入点击短信中的虚假链接填写个人信息，并假冒疾控中心发出验证码让当事人输入，从而套取、掌握当事人个人信息，进一步获取当事人账户、电话控制权，盗取其个人财产。

风险提示：接到疾控人员电话注意识别其身份，辨别真伪。在遇到对方要求点击不明链接，提供个人信息，输入验证码等情况时尤其要引起警惕。建议不明链接不要点，如果收到相关短信，可以在国家卫生健康委推出的“同行密接人员自查”的小程序里先自行筛查判断。

骗局五：“快递涉疫”类诈骗

骗子利用疫情期间市民担心快递可能会传播病毒的心理影响，以“快递被检出新冠阳性、无法送达”为借口，提出“快递虽然会被销毁，但会给快递收件人赔付”的解决方案。之后，诈骗分子通过让当事人扫描二维码或下载 APP 填写快递赔付信息的方式，诱骗当事人透露身份信息、银行账号、短信验证码等，从而控制受害人账户，骗取当事人钱财。

风险提示：此类诈骗类型为“客服退款骗局”，当遇到所谓“客服”通过电话、短信、微信等任何非原购买渠道，声称“快递或订单出现问题进行退款赔付”的，一定不要轻信。此时，应返回原购买渠道，或拨打快递公司官方客服电话，联系工作人员核实情况。切勿轻易扫描未知二维码或下载来源不明的软件、App 等，切勿随意透露个人隐私信息。

骗局六：虚假预约疫苗接种类诈骗

骗子冒充疾控中心工作人员，通过短信发送虚假的新冠疫苗接种信息，引诱受害人点击含木马网址的虚假链接，套取个人信息，伺机实施诈骗。

风险提示：收到含有不明链接的手机短信，请千万不要随意点击。

骗局七：“快速核酸检测”类诈骗

骗子冒充防疫机构工作人员，通过群发“快速出核酸检测结果，加急最快一小时”，“家里也能做核酸检测，只要额外付费便能办到”等信息，吸引某些着急出差、就医等急需核酸报告结果的市民注意，误信骗子能提供服务而添加其微信、QQ等账号。之后骗子引导当事人转账，得手后立即拉黑当事人。

风险提示：全民免费核酸采样时间以社区群通知为准，核酸结果在官方正规平台查询；个人付费核酸采样一定要在经卫健部门认证的具备资质的医院、专业医疗机构或第三方检测机构进行检测，不要轻信网络不实信息和所谓的“私人渠道”；对于转账至不明账户的指令要特别留意，谨防被骗。

骗局八：虚假售卖特效药类诈骗

疫情期间，大家都迫切地希望能出现可治愈或防范疾病的药品。不法分子假冒政府部门或防治新冠肺炎相关部门来电，推销假冒防疫药，或自称是“某国际著名保健品公司中国区代理负责人”，有“秘密渠道”可搞到国外研制、专门预防感染新冠肺炎的保健品，当事人购买“一次服用一辈子都不会感染此类病毒”的良药后，对方迟迟不发货，随后“失联”。

风险提示：事实上，国家相关机构针对疫情研发的所有药品均会通过官方渠道公布，不可能私下联系大家。密切关注官方发布信息，不买、不信任何特效神药，不信非专业机构信息。如果身体出现不适，要第一时间去正规医院寻求帮助。

(三) 披着“疫情”外衣的新型金融诈骗

1、低息贷款型诈骗

(1) 冒充金融平台贷款诈骗

“疫情期间，您缺钱吗？xx金融给您授信1万，申请后马上到账。”随着疫情蔓延，部分老百姓收入减少，资金紧张，一些诈骗团伙开始趁火打劫。他们冒充各大知名金融平台，给用户授信数万额度。但要拿到这些额度，需要缴纳工本费、押金、解冻费等费用几百上千元，很多消费者上当受骗，缴纳费用后再无音讯。

(2) 利用“疫情贷款”诈骗

“您想申请政府疫情专项贷款吗？”疫情期间，不法分子通过电话、网络发布可代理申请“额度高、利息低、无抵押、下款快的政府疫情专项贷款”的虚假信息，诱使有资金需求的公司或个人申请贷款，然后以提前收取中介费、保证金等为由实施诈骗。

真实案例分享：

南京冷冻市场业主王某，近期因需大量进货，手头资金吃紧，恰巧接到一通电话，对方表示可为其办理低息贷款。于是王某根据对方提示，添加“业务员”支付宝好友，并下载了一款“信用贷”APP。

随即，对方提出需缴纳6000元保证金方能放款，王某正准备给对方转账时，南京江宁反诈中心得到线索，立即指令社区民警及时联系王某，告知其立马终止转账，并向他揭露了网络贷款骗局，避免其6000元及后续损失。

应对策略：

申请贷款应当选择银行等合规金融机构，拨打官方电话或前往营业厅办理，拒绝小广告式的网络金融产品。正规的金融机构，不会通过微信等社交软件联系借贷人，沟通办理借贷业务。在放款前不会巧立名目来收取借贷人任何费用，只要是在网上预先交费的贷款业务，一律不要轻信和办理。

2、投资理财型诈骗

(1) 利用“区块链”概念诈骗

不法分子针对在疫情下公众居家防疫、普遍通过网络或手机获取信息的特点，借助“区块链”概念发行冠状病毒加密货币等虚拟货币，宣称筹集的资金用于在境外建造口罩、防护服工厂，或用于研究生产冠状病毒疫苗，并许诺高额回报，骗取受害人钱财。

(2) 伪装成金融机构，利用指导基金、股票、期货等投资诈骗

“宅在家里也能理财”。不法分子利用部分老百姓在疫情期间旺盛的投资需求，通过网络开放平台、微信群向投资人推荐私募基金、指导买卖股票、期货等，引诱受害人下载虚假交易软件并开户投资。

真实案例分享：

2022年2月25日，重庆南岸区公安分局通报了一起数字货币“杀猪盘”电信诈骗案件。

去年年底，热衷投资理财的市民王先生突然被拉进了一个名为“股票投资交流”的QQ群，群里每天都有关于股市“秘籍”讲解的直播链接，而通过学习赚了钱的“同学”隔三岔五就会在群里晒出自己成功赚钱的“成绩单”。

通过一段时间的观察，王先生根据群内提供的链接下载了APP，进入了直播间。每天晚上，直播间都有专业的“导师”进行授课，通过“导师”指导，自己尝试着买的几只股票都赚了钱，尝到甜头的王先生对“导师”愈发信任。

今年1月5日，直播间“导师”在授课过程中，“不经意”间提到自己在投资数字货币，盈利可达2-10倍。1月5日到11日，王先生全家在短短七天时间内陆续向数字货币平台转入180万人民币。接下来的日子，平台内的盈利数据日益飞涨。

但随后王先生发现，这些利润仅仅是平台上的数字，根本无法提现。随后王先生想去咨询“导师”，可发现QQ群、直播网站都联系不上时，才意识到自己被骗，于是来到南坪派出所报警求助。

应对策略：

投资理财应当牢记“高收益意味着高风险”，拒绝高息诱惑。收益永远和风险成正比，面对过高的收益率应保持警惕和理性，切勿存在“天上掉馅饼”的侥幸心理。投资理财应选择正规渠道和合法机构，不要在来历不明的网络平台和APP上投资炒股，那些虚假平台的所谓资金账户，其实就是骗子给你看的数字而已。

3、非法集资型诈骗

(1) 利用为疫区捐款诈骗

不法分子通过虚假网站和微信等社交软件，冒充慈善机构、民政部门、医院、爱心人士等向消费者发送“献爱心”的虚假募捐信息。

(2) 利用感染者亲属众筹“医药费”诈骗

不法分子以孩子或亲属突然高烧、已被隔离医治为由，向社会公众发起众筹“医药费”、“住院费”等，骗取受害人钱财。

(3) 利用“销售返利”诈骗

不法分子利用公众对新冠肺炎的恐慌心理，撒谎称可以代购代销“口罩”、“消毒液”、“特效药”等物资，还向购买者承诺可以“积分返利”，甚至“加盟获利”，骗取受害人钱财。

真实案例分享：

小孙、小蒋经预谋打印虚假宣传材料3000份，在某市多地张贴、散发，假借“市希望工程办公室”“市志愿者协会”之名，以“为抗击新冠肺炎募捐”为由，谎称已联系到口罩等物资的购买渠道，欲欺骗他人向小孙微信账户转募捐款。当日，小孙、小蒋到案。截至案发，尚无钱款转入孙某某微信账户。

黑龙江密山市法院经审理认为，被告人小孙、小蒋以非法占有为目的，在新冠肺炎疫情防控期间假冒慈善机构的名义，以赈灾募捐为由，欲骗取公私财物，情节严重，其行为均构成诈骗罪。小孙、小蒋假借抗疫之名，实施诈骗行为，主观恶性深，社会影响恶劣，应依法从严惩处。小孙、小蒋已着手实施诈骗，因被及时查获而未得逞，系犯罪未遂，可以比照既遂从轻处罚。据此，以诈骗罪分别判处被告人小孙、小蒋有期徒刑十个月，并处罚金人民币

一万元。

应对策略：

正规募捐均需民政部门登记备案，相关信息可通过全国慈善信息公开平台查询。捐款前需核实对方账户名称与受捐公益组织的名称是否一致，不轻易将捐赠资金转入个人账户，避免上当受骗。

4、其他类型的诈骗

(1) 利用“征信洗白”诈骗

“征信洗白，一条 1000 元至 2000 元”“征信修复，修复不成功可退款”网络上，诸如此类的征信修复广告屡见不鲜，声称可以帮助删除或更改征信系统中的不良信息。疫情下，许多人无法按时还上贷款，造成征信有瑕疵，在征信修复骗局中，不法分子主要编造各式“不良信用信息洗白”骗局，教唆消费者无视合同约定，捏造事实，骗取个人钱财，牟取高额费用，侵犯个人隐私。

真实案例分享：

近日，昆明经开区的刘女士在上班期间突然接到一个陌生电话。

“我是京东客服，后台大数据系统监测到您在使用京东白条期间产生了不良记录，现已影响到个人征信，如不及时处理，后果会很严重。”刘女士回想起自己近期确实使用过京东白条，且对方能清楚说出自己的个人身份信息，便半信半疑地向“客服”进一步了解详情。

“客服”取得刘女士的进一步信任后，就在群里发了一个链接，让刘女士点击进去填写一些信息，填写完保存并提交，后台会自动识别。提交个人信息后，对方称相关材料已准备就绪，现只需刘女士向指定银行账户转一笔钱当作“资金验证”费用便可消除不良记录，重置为正常记录。

于是，刘女士分两次转账，合计 511918 元，用来进行“资金验证”。转账成功后，对方声称刘女士的银行卡账户目前存在异常，需进一步验证，此时刘女士认为自己的银行卡不可能存在问题，感觉事情有些蹊跷，便立即向当地派出所寻求帮助，这才发现自己被骗。

应对策略：

“有逾期记录也不用恐慌，一方面，个人信用报告上的逾期记录自欠款和欠息还清后保留 5 年，不会伴随终生；另一方面，银行在做贷款审批时会进行综合研判，不会将信用报告作为唯一参考依据；最后，出现逾期后要及时足额还款，终止不良行为，日常要注意量入为出、合理借贷、按时还款、避免逾期，保持良好的信用记录。

(2) 利用“以房养老”诈骗

正规的以房养老是指老年人住房反向抵押养老保险，即将住房抵押与终身养老年金保险相结合的创新型商业养老保险。拥有房屋完全合法产权的老年人将房产抵押给保险公司，继续拥有房屋占有、使用、收益和经抵押权人(保险公司)同意的处置权，并按照约定条件领取养老金直至身故。长期疫情下导致通货膨胀，部分担心自己的老年生活得不到保障，不法分子伪装成保险公司假借国家政策用“以房养老”名义诱骗老人抵押房产，诈骗资金。

真实案例分享：

2022 年 2 月 19 日，北京市打击对“以房养老”为名的非法集资骗局与陷阱进行了揭底，多起类似案例浮出水面。

例如：北京市民卢女士被熟识的朋友带到一家名为“北京中安民生资产管理有限公司”的宣讲会，被告知只需签订协议，允许将名下的房产抵押给小贷公司，就可以每月领取高额养老金作为回报。同意后，卢女士被对方安排签署了各种协议，也确实收到了“养老金”。但不料几个月后，贷款公司开始上门催债，她被逼卖房还高利贷。

应对策略：

建议消费者尤其是老年人群，在投资产品前，多咨询正规金融机构的专业人员，多与家

人商量，对投资活动的真伪，合法性进行必要的判断和了解，防范不法分子的诈骗侵害，警惕非正规机构疯狂营销揽客行为。

（四）反诈小知识，防骗大锦囊

防骗四句话：陌生电话留心眼，陌生链接不乱点，个人信息保护好，转账汇款多核实。

防骗小知识：

1、要增强证据意识，让对方提供身份证明、产品质量及进货渠道证明，并尽可能地保存好所有与卖方进行联系的证据，如聊天记录、手机短信、转账卡号、转账记录等；发现交易异常情况及时报警。

2、选择货到付款或通过具有第三方正规支付平台的网站进行购买。

3、多关注官方权威报道，了解最新信息，不要听信、传播防疫物资的“小道消息”，增强防范意识。

4、通过正规渠道去购买防疫用品，对陌生身份要审验，在付款之前确认对方的真实性。

5、网络刷单（做任务）本身就是违法行为，所谓网络刷单（做任务）100%是诈骗，不要轻易相信，要通过正规渠道应聘工作，切莫贪小便宜吃大亏。

6、平时接到陌生电话应保持警惕，尤其不要随意向陌生人付费、转账。

防骗常识顺口溜：

冒充银行和电信，欠费透支骗您信；

冒充公安和法院，通过电话来办案；

冒充中介能放贷，冒充专家会理财；

手段纵然千千万，让您汇款都是骗。

公安部、工信部、中国人民银行等部门联合构建推出了“五大反诈利器”——国家反诈中心 APP、96110 预警劝阻专线、12381 涉诈预警劝阻短信系统、全国移动电话卡“一证通查”服务、云闪付 APP “一键查卡”。

（五）有奖竞答

准备了五道题目大家猜猜看，答对可抽取小礼品哦！

1、假如你是小明，已遭遇利用疫情进行诈骗的情况，你会怎么处理？（C）

A.自认倒霉，下次提高警惕。

B.已了解这些诈骗套路，下次再遇到可与骗子周旋，以其人之道还治其人之身。

C.打电话报警，提供相关信息给警方。

2、假如你接到自称是某宝客服电话，能说出你的名字和购买物品，告知你的快递因检测出阳性需要销毁，让你点进一个链接登记资料进行理赔，你会怎么做？（BC）

A.能了解这么详细信息的应该不是诈骗，根据对方提示，点开链接进行登记。

B.挂断电话，找商家核实快递情况再处理。

C.是诈骗，不予理会。

3、你收到一条尾号是“95588”的陌生号码发来的短信，说你的电子银行密码已过期，需要登陆网站进行操作，系列做法正确的是？（D）

A.点击短信里的网站链接，按照提示操作“升级”。

B.置之不理，删除短信。

C.向家人或者朋友求助真伪。

D.报警或向银行部门官方电话求证，发现诈骗网站，对垃圾短信进行举报。

4、接到要求转账和索要验证码的电话，下列哪个做法不正确？（C）

A.及时与发卡银行客户服务专用号码联系鉴别通知真伪。

B.先谨慎核对其身份和账户名。

C.“宁可信其有，不可信其无”，按电话指示做。

5、以下哪些是反诈利器？（ABCDE）

A.国家反诈中心 app

B.96110 预警劝阻专线

C.12381 涉诈预警劝阻短信系统

D.云闪付 app"一键查卡"

E.全国移动电话卡“一证通查”服务