

某200元购买装备，350元卖出，提现顺利。几天后，陆某1200元购买装备，1600元卖出，提现顺利。一周后，陆某2500元购买装备3500元卖出，提现显示操作错误被冻结，需缴纳5000元押金，客服人员帮助解冻后退回，缴纳押金后陆某被拉黑。

3、网络刷单。某同学帮电商刷单，给佣金。例如，先刷一笔100元，返佣金15元；再刷一笔300元，返佣金50元；再刷5000元，被拉黑。

4、非法网络购物。杨同学通过抖音等平台加陌生人微信，关注一段时间后陌生人向杨同学介绍一款购物返现的APP，每500元购买一个账号用于购物返现（例如花100元购买一箱方便面，收到快递后，返现120元），使用一段时间后该同学向家人、朋友介绍这款APP，多人使用一段时间，投入几千至几万元后不能提现。经公安机关鉴定该APP涉嫌网络洗钱、涉嫌网络传销、涉嫌网络诈骗。

5、虚假投资理财诈骗。陈同学在朋友圈看到一篇关于炒股的文章，感觉写得很好，就添加了文章里发布的微信，对方邀请陈某进入炒股精英群。一个“股票导师”在群里进行荐股和行情分析，陈某看了几天后，发现群里的人按照“导师”的分析都赚钱了，蠢蠢欲动试水投资，几次尝试后都赚钱了，随加大投入。在两周时间内，陈某通过网络贷款、家人借钱陆续投入3万余元，但在提现时一直无法成功，发现被骗。

6、其他。常见的网络诈骗手段还有“杀猪盘”诈骗、网络贷款诈骗、冒充熟人或领导诈骗、冒充“公检法”诈骗、注销“校园贷”诈骗等。

## （二）网络诈骗特点

和传统的诈骗犯罪一样，网络诈骗也是以传播虚假的事实、信息为手段，以非法占有他人的财务为目的。但与传统的诈骗犯罪行为不同的是，网络诈骗是以互联网作为实施犯罪行为的平台。<sup>[5]</sup>随着社会的发展，网络诈骗的各种手段也是层出不穷。大致来说，校园网络诈骗具有如下的几个特点：

1、诈骗手段多样化。从被骗学生情况可以看出，嫌疑人实施诈骗的手段非常丰富多彩，甚至有一些是针对大学生群体的方式方法。如兼职招聘、买卖收购游戏装备等，尽管各级组织都在加强教育，但是新的网络诈骗手段仍不断出现，让学生防不胜防。

2、施诈者身份高度隐蔽。互联网的虚拟性使施诈者容易隐蔽身份，有些冒充“公检法”，有些利用服务器架设在境外进行诈骗，身份随机变换，难以识别、难以追踪。

3、施诈者团队专业化。从虚假买卖、冒充客服、虚假投资等案例看，施诈者精准把握大学生的心理状况，不再是一个或者几个人开展，而是从联络、客服到金融账号构成链条完整的专业化团队。

4、网络诈骗危害更大。网络诈骗不仅可以骗到有余额

的同学，还可以诱导困难生通过网络借贷等方式被骗，导致困难生家庭雪上加霜，甚至被迫休学。

## 大学生被网络诈骗原因分析

经与被骗学生一对一深度访谈，向宿舍、班级同学侧面了解，结合2020年《新形势下电信网络诈骗治理研究报告》，某高职院校被骗学生主要特点有：

1、几乎所有被骗同学都有贪图小便宜的念头，都存在侥幸心理，明明怀疑自己正在被骗，还要天真的以为自己“运气好”，遇到赚钱的机会了。

2、学生社会经验不足，防范意识差，容易轻信别人，法律意识淡薄。

3、日常消费以网络购物为主，在网购中退货换货相对比较频繁。

4、不少同学沉迷于网络游戏，在虚拟的游戏中有相当一部分未曾见面的游戏伙伴，确有深度信任感。

5、错误认识网络诈骗，认为自己没钱，就不是诈骗者的目标。盲目自信，认为自己不会被骗，所有的诈骗手段都可以轻易识别，因此对学校、辅导员等老师的防诈骗教育视而不见。

6、同学之间交流少，不及时向师生验证。遇到不确定自己是否被骗时，不和同学交流，不敢向老师求证，只能默默的自己猜测。

## 多方联动有效应对大学生网络诈骗措施

根据某高职院校被诈骗案例，结合2021年开展防范网络诈骗教育和相关工作实际，组建校-院-班-舍的纵向防范网络诈骗队伍，举办诈骗案例通报、防诈骗主题班会、防诈骗能力测试、防诈骗情景剧演出等多项活动，形成“九个一”的高职院校防范网络诈骗经验。

1、分层组建一个防诈骗工作交流群。在校-院-班-舍四个层面组建防诈骗工作交流群，及时将诈骗案发情况和具体案情进行通报，推送反诈视频、文章等内容，将反诈信息第一时间流转每位师生。

2、关注一个防诈骗公众号和注册小程序。责任到人100%全覆盖安装“国家反诈中心”官方APP，关注“国家反诈中心”公众号。

3、举办一场防诈骗专题讲座。邀请诈骗公安民警举办防诈骗专题讲座，进行典型案例剖析及防范指导，及时向师生提供最新的反诈资讯。

4、签订一份个人防诈骗倡议书。所有同学签订防诈骗倡议书，课间集体朗读国家反诈中心总结的10条常见诈骗手段，不断加深印象，提高防诈骗能力。

5、开展一次防诈骗知识测验。通过“易班”APP，组织广大学生进行一次防诈骗知识测验。对考试不合格者，专人辅导，直至人人过关。