

抛出高薪诱饵，锁定求职者

上海警方“净网2019”专项行动破获涉网违法犯罪案件1800余起 抓获3500余人

□法治报记者 季张颖

当前，传统违法犯罪正加速向以电信、互联网等为媒介的非接触性犯罪转移，借助网络的新型犯罪日益增多。昨天，上海警方召开“净网2019”专项工作新闻发布会，通报上海警方“净网2019”专项工作整体情况及典型案例。记者从会上获悉，今年以来，上海公安机关根据公安部统一部署，深入开展“净网2019”专项行动，严厉打击网络违法犯罪，努力构建文明有序的网络空间。

专项行动以来，全市公安机关破获各类网络诈骗、黑客攻击犯罪、侵犯公民个人信息犯罪、网络赌博等涉网违法犯罪案件1800余起，打掉涉网犯罪团伙53个，抓获违法犯罪嫌疑人3500余人，依法处置违法违规网站262家（次）。

【案件一】 高薪诱饵招工设下“连环套”

“足不出户在家轻松月入过万，加QQ私聊……”今年1月，市公安局网安总队在工作中发现，有不法分子过“IS语音平台”、“YY语音”等社交软件的公共聊天板块中发布这样一种诱导招工信息。

警方经进一步调查发现，该招工信息是一个以何某为首的诈骗团伙发布的虚假信息。该犯罪团伙有17名成员，由何某统一指挥，其中有“介绍人”、“指导老师”、“一对一指导老师”、“返现老师”、“老板”等5个层级，以承诺向求职者提供不同质量的工作为由，通过“连环套”的形式向被害人收取不同等级的会员费进行诈骗。

市公安局新闻办新闻发言人助理庄莉强介绍，在这样一种运作模式中，首先，“介绍人”会在网上批量发布虚假招工广告，并将有求职意向的被害人推荐给“指导老师”。随后，“指导老师”和被害人联系后表示，需交99元成为会员后按照会员待遇介绍相应工作。

“待被害人交钱后，‘指导老师’就会继续忽悠，99元的普通会员只会提供一些兼职的工作，按天结算工资，并表示每介绍一个兼职工作前由被害人先行垫付149元。如果被害人觉得不合适，那么需再支付139元高级会员费，由‘一对一指导老师’介绍更好的工作。”

一般被害人都会选择支付139元高级会费，此时“一对一指导老师”便出场了。他们与被害人联系时仍然避而不谈工作，而是交给被害人一个任务，称完成这个任务后既可以有更优质的工作机会，更可以获得现金返利。

17人团伙5个层级各自抽成

此时，便是“返现老师”登场的时候。他会要求被害人实名办理10张38元的“中国移动流量卡套餐”，完成即可返还前期所有手续费。然而，这些犯罪嫌疑人很清楚，中国移动对同一实名用户办理注册的手机卡数量有限制，因此，被害人是无法完成这个任务的，接下来犯罪嫌疑人一方面会等待被害人提供部分手机卡号，之后便会拉黑被害人销声匿迹。

最终，这个犯罪团伙诈骗的钱财会统一汇入“老板”何某的账户。何某每日结账，给不同层级的团伙成员分配相应的赃款。比如，99元会员费中，“介绍人”抽成60元，“指导老师”抽成20元，其余归何某；139元会员费中，“介绍人”抽成60元，“一对一指导老师”抽成23元，其余归何某。“返现老师”则通过出售手机卡与何某分赃。

记者从采访中获悉，自今年1月起到案发，该团伙累计诈骗达8000余次，涉及全国15个省市，涉案总金额约200余万元。其中，团伙主犯何某还曾供职于某人才交流市场，熟悉并了解企业招聘、涉外劳务输出的工作经验，其余的所谓“老师”都是何某通过朋友圈、老乡圈搭识的，为20至30岁不等的年轻人，他们为了骗取钱财而聚在一起导演了这场招工的骗局。

4月3日凌晨，市公安局网安总队会同宝山分局在全国13个地级市统一行动，抓获包括团伙主要犯罪嫌疑人何某在内的犯罪嫌疑人17人，一举捣毁该利用互联网实施招工诈骗的犯罪团伙，并当场缴获了作案用手机、电脑、U盘等大量涉案工具。

目前，何某等3人因涉嫌诈骗罪已被依法批准逮捕，其余犯罪嫌疑人被依法采取刑事强制措施，案件在进一步侦查中。



■ 警方声音

指导3500余家企业开展风险评估 互联网信息服务“装好刹车再上路”

网安总队党委委员、指挥室主任陆明介绍，面对复杂而严峻的网络犯罪形势，上海公安机关主动作为，积极探索行之有效的整治措施。在重拳打击犯罪方面，上海警方坚持“打集群、打平台、打团伙、打幕后”的工作思路，全链条、全方位打击突出网络违法犯罪，最大程度挤压网络违法犯罪活动空间。

同时，为进一步加强网络安全执法检查力度，上海警方对联网单位是否落实公安备案、安全评估、公民个人信息保护等网络安全管理要求还进行了专项检查，全面提升互联网企业落实安全管理主体责任的自觉性。

其间，上海警方还联动社会共治，组织本市具有论坛、聊天室、通讯群组、音视频、网络直播等信息服务的网站及APP运营企业开展安全风险自评

工作，指导3500余家企业提交评估报告4000余份，确保互联网信息服务“装好刹车再上路”，共同形成对打击网络违法犯罪的高压态势。

“在我们侦办的案件中，我们还发现网络诈骗类案件高发，截至5月底，上海共侦破网络诈骗案件950余起，这类案件中尤其是网上购物、网上兼职、虚假网贷、网络交友、虚假网游以及冒充熟人等类型的网络诈骗突出，这几类网络诈骗占到所有网络诈骗的8成以上。”

陆明透露，上海公安机关将进一步强化网络诈骗的依法查处和预警防范工作，结合本市多发网络诈骗类型特点、受害人群特点等强化预警提示，通过新媒体平台发布防范博文和视频作品，不断提升广大市民的防范意识。

【案件二】 理财群里的“角色扮演”

另一起典型案件发生在上海青浦。今年1月，市民黎女士报案称：2018年12月中旬，自己被陌生好友拉入一个投资理财群，按照陌生人的指引在“51bit”的投资软件上进行投资理财后被骗5万元，上海警方接报后立即展开调查。经查，市民黎女士加入的投资理财群系一诈骗团伙组建，阳某、康某为该团伙的主要犯罪嫌疑人。

青浦分局网安支队民警告诉记者，这个犯罪团伙的行骗工具主要为一款名为“51bit”的虚假投资软件，并在这款软件上投放了“柚子币、摩根币、亚洲币”等所谓投资理财产品。之后，犯罪嫌疑人阳某等人通过拨打电话推销“51bit”理财产品的方式，物色对投资理财感兴趣的被害人，随后添加被害人为微信好友，并拉进犯罪嫌疑人康某开设的所谓投资理财微信群。

那么，该犯罪团伙是如何利用投资理财微信群进行诈骗的呢？原来，该微信群自组建起，就玩起了角色扮演的游戏。由犯罪嫌疑人康某扮演专业“理财讲师”，由其他团伙成员以不同身份扮演对投资理财感兴趣的“群成员”角色，每个微信群内有60-70人，分别由6-7个团伙成员操控，每个成员注册并操控8-10个小号，共拉1-2个被害人进群。

略涨后一路跌至亏光

接着，为了忽悠被害人投资理财，他们使用“专业”的话术剧本进行诈骗活动。由“理财讲师”在群内不断吹捧理财投资股票及虚拟货币产品，由“群成员”或冒充投资理财高手发表理财经验，或冒充投资理财的“小白”咨询各种问题并期待理财产品的高收益等等。

经过一段时间的经营，骗取了被害人对该产品的信任后，“理财讲师”便带着大家“发财致富”为借口，耐心指导被害人安装注册“51bit”的投资软件，并向一个私人银行账户转账进行投资。待被害人投资成功后，“理财讲师”就变成了“皇帝的新装”故事中的“裁缝”，假模假样地指导被害人在该软件内进行所谓的专用虚拟币种操作。

办案民警告诉记者，这些以虚拟币为名的投资理财产品其实都是他们随意编造出来的，并未在市场上实际流通过。“起初会有略微涨幅，可是没过多久便一路下跌，待被害人的投资金额被其操控至全部亏损时，便会拉黑被害人，并解散微信群。”截至案发，该团伙共骗取钱财约60万元人民币。

3月20日，青浦警方奔赴广东省深圳市龙岗区开展抓捕行动，抓获犯罪嫌疑人38人，当场查获作案手机100余部、电脑50余台、电话机30余部，诈骗用话术本数本。

目前，7名犯罪嫌疑人因涉嫌诈骗罪已被青浦区人民检察院依法批准逮捕，其余31名犯罪嫌疑人也已被青浦警方依法采取强制措施，案件正在进一步侦查中。