以不特定人群为目标实施电信诈骗

小心！不要落入“杀鱼盘”陷阱

网络诈骗中有一个专属名词叫“杀鱼盘”，它遵循了网络诈骗广撒网的特点，分别由提供技术支持并负责洗钱分赃的“船长”、寻找受害人并引导付款的“渔夫”以及被害人“鱼”构成，完成“杀鱼”即行骗成功。

近年来，一些不法分子在二手交易平台以低价吸引买家，然后诱骗买家离开平台，通过他们提供的虚假链接付款进而诈骗钱财。由于链接页面和正规平台页面很相像，极具迷惑性，买家几乎很难察觉，极易落入这种网络诈骗的“杀鱼盘”中。“杀鱼盘”是一种以不特定人群为目标的电信诈骗案件，不同的是，“杀鱼盘”的诈骗金额较小，针对的目标人群还经常包括未成年的学生。

资料图片

案例—1 一旦付款，立即被拉黑

去年 10 月 15 日，江苏常州武进的消费者小马在二手平台购买相机时，遭遇“杀鱼盘”后报警。

小马在某二手交易平台遇到了一个卖二手相机的卖家，卖方建议微信详谈。讲好价钱后，对方发来一个付款链接。小马打开链接后发现确实为先前浏览过的二手平台支付页面，于是爽快地付款。然而，货款到账的下一秒，他发现自己已被卖家拉黑。

警方围绕嫌疑人微信和 QQ 号信息展开梳理分析，最终确认在河北的易某有重大嫌疑。去年 11 月 2 日，警方奔赴河北，成功抓获犯罪嫌疑人易某。

易某交代，自己是在一个 QQ 群中认识了“上线”，这个“上线”教他如何利用虚假购物链接赚外快。两人分工明确，易某负责寻找下手对象，谈妥价格，“上线”则负责将虚假支付链接发给易某，诈骗成功后，每单易某可分到七成。

通过对“上线”与易某的聊天内容、钱款转账等信息的分析，警方进一步锁定了这名嫌疑人的真实身份。去年 11 月 15 日，何某在居住地被抓获。

通过对何某社交软件上的关系人、银行账户资金流以及信息流等情况的深入研判，警方发现，何某手中有着像易某一样角色的下线和同行“船长”各 10 余人，一个冒充二手购物平台、制作虚假链接实施网络诈骗的犯罪团伙进入了警方的视野。去年 11 月，该团伙成员全部被警方抓获。

去年底，犯罪嫌疑人易某因涉嫌诈骗罪被批捕。从去年 12 月 2 日至今年 1 月 21 日，全案 19 名嫌疑人陆续被提请审查批捕。

案例—2 小心“花呗提额”诈骗

“大幅提升花呗、借呗额度不是梦”，看到这样的广告可要多个心眼，这或许真是一场“黄粱梦”。去年 11 月初，市民张先生在浏览网页时，一条“大幅提升花呗、借呗额度”的广告信息引起了他的兴趣，并与之联系。然而，对方告诉张先生需要验证他的还款能力，必须要在他的银行卡里存 12000 元才能提额。存款完毕后，对方又发来一个网址链接，让张先生填写自己的银行卡号、密码和手机验证码。急着用钱的张先生没多想，便按此操作，紧接着他的手机就收到扣款短信，自己也已经被“拉黑”了。

合肥市公安局反电诈中心民警朱云龙告诉记者，像这种诈骗手段被骗子称作“杀鱼盘”，“钓鱼手”在社交、游戏等网络平台发布虚假广告，骗得“鱼”也就是受害者的信任，然后把“鱼”交给“杀鱼手”来具体实施诈骗，其大多以服务费、手续费名义让受害人转账，或验证还款能力等为由发送假链接盗刷资金。

警方提醒广大民众，要求提前交纳手续费、服务费等各种费用的贷款一定是诈骗，小心落入此类“杀鱼盘”的圈套，任何网络传言的提额方式，如提供账户信息、转账、扫描指定二维码等都是诈骗，陌生的网址链接和二维码切记不要点击扫描，一旦发现被骗，应保存好证据，尽快报警。

案例—3 小学生成“杀鱼盘”诈骗目标

小丽是黑龙江齐齐哈尔市建华区一名小学五年级学生，小小年纪的她怎么也想不到，电信诈骗会落到她头上，而且是从一个刚刚添加的陌生网友开始的。小丽告诉记者，“网友说他过生日，只要给他发 888.88 元红包，就给我返 8888.88 元。我看他朋友圈有两三个人的类似截图，我就相信了。”

小丽将第一笔钱 800 多元，按那个网友要求转了出去，可是五分钟过去了，小丽什么也没收到。此后，该网友说银行卡有限额，让小丽再给他 400 多元。发完之后，网友让小丽等 10 分钟，说待会儿就把钱转给她，两人语音通话了 10 分钟，10 分钟后对方就突然挂了，并把小丽拉黑了。

由于被骗的 1000 多元是小丽攒的压岁钱，小姑娘很心疼，更怕父母知道责怪她，她盯着那个微信号看了半天，忽然发现几个字母后面，明显就是一个 185 开头的手机号，小姑娘试着拨通了那个电话。

机敏的小丽与对方在电话中周旋了 40 多分钟，并得到了对方的住址、身份证号码等信息。第二天，在家人的陪同下，小丽拿着所有的证据和对方的资料到公安机关报案。

齐齐哈尔市警方接到报警后，迅速对这起案件展开调查。根据小丽提供的信息，当天就确定了三名嫌疑人的真实身份。就在警方开展调查的同时，其中两名嫌疑人的账户还在不断地收钱。

在三地公安机关的配合下，成功将 3 名嫌疑人抓捕归案。经分别突审，江西、安徽两地嫌疑人交代，他们只负责收钱转账，而广东嫌疑人则是把他自己的微信号以每天 200 元的价格租给他人使用。

通过对这 3 名嫌疑人的审讯，他们同时供出了一个叫何某的人，这个何某成为了最大的嫌疑人。经过进一步工作，警方掌握了何某的真实身份及行动轨迹，6 月 10 日，抓捕组在江西鄱阳县一网吧将嫌疑人何某抓获。之后又陆续抓获其他 5 名团伙成员。

嫌疑人交代，“杀鱼盘”针对的被害人群体主要是中小学生，年龄小、社会经验少、分辨能力比较差、容易上当受骗，而且被骗之后一般都不敢告诉家长，大部分也就不会报案。

如何认定犯罪金额？

普通电信网络诈骗通常是点对点的打款方式，然而在“杀鱼盘”中，被害人的钱款并非直接打入被告人的账户中，而是购买了电商平台的电子购物卡。

记者了解到，在上述二手交易的“杀鱼盘”案中，被告人提供的钓鱼网站链接打开后，与真实的二手购物平台网站极其相似，被害人难以分辨。但点击付款后，钓鱼网站则会通过事先抓取的接口链接到某购物平台，被害人的付款会被用于购买该购物平台的购物卡。

通过核查被告人与被害人的聊天记录、诈骗团伙上下线之间的聊天记录、被拉黑的被害人账号以及被告人的购物平台账号的订单等信息，承办检察官核实到该案涉及 400 余名被害人。但由于被告人使用的各种社交软件账号和购物平台账号均为购买的“小号”，并非实名，所以大量被害人信息无法准确核实。

在被害人“缺失”的情况下，该案中被告人之间的转账记录是否还能被认定为犯罪金额呢？

承办检察官告诉记者，被告人的账户确为诈骗所得、电商平台的账户订单确为他人付款购买，且通过全案证据排除了上下线其他经济往来，排除合理怀疑，再综合已查明的被害人陈述、交易记录、电子数据等，足以证实“违法来源”的排他性。因此，承办人最终将上下线转账记录认定为犯罪金额，该案涉案金额总计达 100 余万元。

脱离正规平台易踩“雷”

据 2020 年《法治蓝皮书》，电信网络诈骗仍呈高发趋势，且运作模式呈现更加明显的专业化、集团化趋向，犯罪分子的犯罪手段也越来越智能化，电信网络诈骗犯罪集团逐渐形成恶意注册、引流、诈骗、洗钱等上下游环节勾连配合的完整链条，也形成了电信网络诈骗的“新范式”。

在武进区人民检察院办理的电信网络诈骗案例中，除了通过低价二手交易进行诈骗的“杀鱼盘”之外，还有以投资理财为名设“杀猪盘”实施诈骗、以网络刷单返现实施诈骗、以裸聊为饵通过 APP 软件非法获取用户信息后实施诈骗或者敲诈勒索、在婚恋网站交友实施诈骗、以办理贷款为由设各种名目要求缴纳保证金实施诈骗等类型。

据介绍，这些电信网络诈骗的受害群体广泛，作案手段也更为隐蔽，犯罪分子往往潜伏在各大论坛、贴吧和购物平台，先在正规平台寻找“猎物”，再诱导受害人脱离平台转到微信或者 QQ 上，点击由他们提供的“高仿”网站链接进行交易。

为此，专家提醒，无论是网络购物还是网上交友，一定要选择正规平台，使用平台提供的交流系统进行沟通和交易，凡是绕开平台由陌生人提供的来路不明的 APP 软件或者网站链接、二维码，不要轻易点击下载和注册。同时，各大电商平台也要加强网络安全防范，有效提示和拦截站外钓鱼网站，强化技术升级，严防犯罪分子抓取链接制造“高仿”网站，对可疑违法信息应进行屏蔽或封号等，从源头上维护网络环境安全。

（综合《工人日报》、央视财经等）