

诱导买家在虚假链接付款 当心二手交易平台“杀鱼盘”

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。

不法分子嗅到“商机”

如今,不少消费者通过二手交易平台将闲置物品转给别人,这样既可以让闲置物品循环利用,又能让自己赚点零花钱,但这也让不法分子嗅到了“商机”。

记者近日采访了解到,利用二手交易,诱骗买家私下联系并点击虚假链接付款,这种网络诈骗有一个专属名词叫“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”以及在二手交易平台淘货的被害人“鱼”构成,完成“杀鱼”即行骗成功。

付款后就被拉黑

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。从2019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。

大量被害人信息难核实

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“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”

新型电信网络诈骗层出不穷,“套路”之多让人防不胜防。

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“新模式”。

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。(工人日报)

警惕“短信嗅探器” 窃取钱财

记者27日从河北省唐山市公安局海港经济开发区分局了解到,警方成功捣毁了一个使用“短信嗅探器”流窜作案的电信诈骗团伙,抓获犯罪嫌疑人8名,涉案金额10万余元。

“随时随地获取他人信息”“无需对方任何操作即可盗取钱财”……这看似不可能的诈骗是唐山警方在捣毁一个电信诈骗团伙时,嫌疑人的亲口供述。而在抓捕现场,一同缉获的便是达成上述不可能的工具——“短信嗅探器”。

警方调查发现,随着科技的提升,信息拦截设备也逐渐被不法分子利用。一些人在受害人夜间熟睡时使用短信嗅探设备,便可在不惊动受害人的情况下截取用户手机短信内容。随后,利用网站、移动支付等存在的技术漏洞和缺陷,窃取个人信息、银行卡号,使用支付平台绑定其银行卡,截取短信验证码,随时盗刷资金。

民警提醒,“嗅探”式电信诈骗虽然隐秘,但也不是无法防范,取消银行卡免密支付,夜间睡觉时关闭手机等均能让“嗅探”失灵。(据新华社)

小伙“挑战酒驾” 1分钟后车祸身亡



近日,北京海淀区27岁小伙小王和同事聚餐饮酒后,本已经找好了代驾,将一名同事送到家后,小王居然直接结账并将代驾赶走,还拿出手机录视频,拍摄了车上另外两名醉酒的同事,并发出“豪言”：“挑战北京酒驾”。

0时54分,视频拍摄完毕,通过微信发给了朋友。可想而知,朋友看到后多么着急。“你别开车”“你找代驾”“我求你了”,朋友先后两次发起了语音通话。只可惜,0时55分,事故就已经发生了。

0时55分,海淀区永丰路,小王醉酒驾驶的小轿车由北向南行驶中,车辆驶出道路与路东侧围挡及井台相撞,小王当场死亡,车内1名同事受伤。(北京日报)