

上午下单购物,下午诈骗电话就来了 谁是冒充客服实施诈骗的“黑手”?

上午下单购物,下午诈骗电话就来了,谁在给诈骗分子提供网购信息?这边钱才转出,那边已购游戏点卡、数字预付卡,谁在帮诈骗分子洗钱?每次诈骗都要换号,诈骗团伙哪来那么多微信号、QQ号?

从去年5月到今年4月,江苏省宿迁市公安局对“5·15”系列冒充客服诈骗案实施全链条打击,隐匿在网络诈骗背后的“黑灰产”面纱被揭开。



“精准下套”新华社发 商海春 作

卡上没钱 照样被骗走近5万元

2019年4月28日,苏州的郑女士突然接到一个电话,对方自称是支付宝理赔中心的。在核对郑女士的手机、地址信息后,对方说,她在淘宝买的内衣快递丢失,现予以赔偿;丢失商品价格为62元,理赔162元。

郑女士头天确实是在淘宝上购买了内衣,价格正是62元。所以,她没有怀疑,再加上自己卡里也没多少钱,就按照对方要求和引导,加了微信,扫了对方发来的二维码,填写了银行卡信息,还用支付宝账号登录了一个贷款应用程序,结果稀里糊涂贷款5万元。

4月29日,5万元贷款到账,进入郑女士支付宝账户。她感觉不放心,就提现到银行卡里。不料几分钟,她就收到短信,卡里的钱被转出49950元。郑女士随后到附近派出所报警。

郑女士被骗后不久,宿迁市公安局破获一起种植木马病毒、盗窃淘宝商户网购订单数据的案件。警方查获数以百万计的被盗网购信息,郑女士的网购信息也在其中。警方调查发现,郑女士正是因为网购信息被盗,继而成为网络诈骗的受害者。

“在网络诈骗背后,到底隐藏了哪些‘黑灰产业链’?”宿迁市公安局副局长陈红淦说,带着这一疑问,宿迁警方对此案实施全链条打击,最终摧毁6个诈骗团伙,抓获各环节犯罪嫌疑人共29名,查扣网购订单数据等公民个人信息2500余万条、QQ账号460余万个、微信账号10余万个。

“1个骗子11个帮”:贪图小利助纣为虐者不少

记者最近来到宿迁,采访相关办案人员了解到,在1个网络诈骗分子的背后,竟然有11个人在帮其实施犯罪。

以郑某诈骗团伙为例,这一诈骗团伙是宿迁警方此次摧毁的6个诈骗团伙之一,隐匿在中缅边境,冒充快递公司或电商平台的客服打电话给受害人,以快递丢失、商品存在质量问题为由,主动提出理赔,继而一步步诱使受害人落入圈套。

诈骗团伙如何知道受害人购物了?宿迁警方查明,处于诈骗链上游的是“料商”,他们为诈骗团伙提供网购订单数据。

郑某诈骗团伙的“料商”是2名杨姓犯罪嫌疑人。他们通过“内鬼”,或者将有关木马病毒

植入商户电脑,盗取商户每日出售、寄递商品信息,再转卖给诈骗团伙。信息越“新鲜”价格越高,最高一条能卖6元左右。

参与诈骗的犯罪嫌疑人张某向记者坦言,“料商”让诈骗成功率更高;他每天打50至100个电话,一个月能骗到十五六个人,最高一单骗了29万元。

诈骗团伙如何隐匿资金?宿迁警方查明,处于诈骗链下游的是“卡商”,他们负责为诈骗团伙洗钱。

所谓“卡商”,即游戏点卡或数字预付卡回收倒卖商贩。为郑某诈骗团伙提供洗钱服务的共有5人,1人为中间人,2人是Q币回收倒卖商贩,2人为苏宁卡回收倒卖商贩。一旦诈骗

得逞,郑某诈骗团伙会立即用诈骗所得购买Q币或苏宁卡,有时直接诱骗受害人扫码购买Q币或苏宁卡;然后交由中间人处理,中间人再找“卡商”变现。

宿迁市公安局刑警支队副支队长夏学建介绍,调查表明,2019年4月底至6月初,2名苏宁卡回收倒卖商贩以九七折回收苏宁卡,为郑某诈骗团伙洗钱300余万元;2名Q币回收倒卖商贩以八六折回收Q币,为郑某诈骗团伙洗钱200余万元。

每次诈骗都要换号,诈骗团伙哪来那么多微信号、QQ号?宿迁警方查明,“号商”是诈骗工具的重要来源。

为郑某诈骗团伙提供诈骗工具的“号商”共4人,其中2人是微信“号商”,2人是QQ“号商”。据4人交代,在他们背后,又有专门团伙或技术人员为其提供批量注册、养号等服务。普通微信号每个售价10元左右,使用年限特别长的实名号,一个能卖到200元;普通QQ号一个能卖到10元甚至数十元——令牌号难以查封,诈骗分子更加偏爱。

陈红淦说,网络诈骗还在不断变异,分工越来越细化,人员流、资金流、信息流越来越复杂,每个环节都滋生出一条“黑产”或“灰产”,这种态势值得警惕。

遏制电信网络诈骗重在协同治理

据了解,今年以来,网络诈骗依然呈现高发态势,其中网络诈骗发案量居第四位。

深入剖析“5·15”系列冒充客服诈骗案,办案人员认为,网络诈骗猖獗,关键在于一些监管政策、法规未能得到贯彻落实。

“电话卡滥发是个重要原因。”夏学建说,“不法分子实施诈骗,第一件事就是打电话,其电话卡从何而来,实名制落实了吗?警方在‘号商’陈某电脑中查获微信账号10余万个,查明其出售微信账号30余万个;

在‘号商’周某电脑中查获QQ号460余万个,其中令牌号37万个,查明其出售QQ号近千万个。绑定这些微信号、QQ号的电话卡又从何而来?”

夏学建介绍,本案中,警方溯源发现,至少21家移动转售企业未能依规经营,21家企业全部违反专用号段规定违规开设行业用卡,全部违反业务功能限制规定开通短信功能,9家未尽审核责任为同一用户大量开卡。

其次是网络服务公司未能依法经营。办案人员分析,一

些社交软件之所以成为诈骗分子的诈骗工具或引流工具,就是因为没能将实名制的相关规定落到实处,或者没有严格执行相关法律法规。

三是企业大量获取公民信息,却又疏于内部防范。宿迁市公安局刑警支队办案民警胡宏斌介绍,本案中,“料商”主要通过“内鬼”或植入木马程序盗取网购订单数据。不管是“内鬼”盗取还是木马程序盗取,均表明相关电商平台和商户对客户信息保护没有给予足够重视,内部防范措施不到位。

四是网络空间违法信息泛滥。一些涉案犯罪嫌疑人说,诈骗、洗钱、养号所需工具,在网络空间均可轻易获取;比如注册账号时需要验证码,如果不想输入自己的手机号,只要搜索接码平台,就有大量平台可提供验证码接收服务。

办案人员呼吁,遏制电信网络诈骗犯罪,仅靠公安机关打击是不够的,关键在网络空间协同治理;有关部门要形成合力,督促相关企业落实政策法规,彻底清除诈骗滋生的土壤。(据新华社11月9日电)