

民有所呼 / 我有所应

点题·爆料邮箱: mssd@xmwb.com.cn 线索一旦采用 即付稿酬

“网骗”已成中国第三大黑色产业

前三季度上海人网上受骗上当人均损失最大



据国内首个网络诈骗全民举报平台——猎网平台最新公布的数据显示:基于对今年以来网民举报的近9万起网络诈骗案件的追踪研究发现,目前国内网络诈骗已形成了一条完整的、分工明确的地下黑产业链,可划分多达15个“工种”。初步统计,网络诈骗从业者至少有160万人,“年产值”超过1100亿元。

《现代网络诈骗产业链分析报告》透露:今年1-9月,共接到全国网民举报网络诈骗案件20086起,涉案金额高达8901万元,人均损失4431元。如果按照城市人均损失划分,上海以人均损失8084元位列全国第一。

黑产业链从业者或超过160万

“这还只是估算了诈骗电话所对应的产业规模,对于短信诈骗、网页诈骗、QQ诈骗等多种其他网络诈骗方式,都还没有计算在内。”猎网平台反网络诈骗专家裴智勇认为,网络诈骗地下产业已列中国第三大黑色产业。

猎网平台追踪过去3年间网民举报的89484起网络诈骗案件,发现即便是手法最简单的网络诈骗,也至少需要10人的犯罪团伙。从开发制作、批发零售到诈骗实施、分赃销赃,网络诈骗可划分出多达钓鱼编辑、木马开发、盗库黑客、电话诈骗经理、短信群发商、在线推广技师、财务会计师等15个不同“工种”。《报告》显示:今年前三季度,仅360手机卫士就为用户识别和拦截诈骗电话43.7亿次,平均每天识别和拦截诈骗电话1601万次。“若按照每个诈骗电话经理平



图 CFP

均每天可拨打100个诈骗电话计算,拨打1601万次诈骗电话至少要有16万名诈骗电话经理。裴智勇分析说,按每个诈骗电话经理对应10个产业链从业人员计算,16万名诈骗电话经理的背后就有160万名网络诈骗从业者。以人均月收入6000元推算,160万从业者的“年产值”至少为1152亿元。

打击难度较大 因为取证困难

据悉,网络诈骗地下产业规模之所以迅速扩大,主要是由于网络诈骗犯罪打击难度大,具有异地作案、小额多发、取证困难等特点。骗子往往与受害者不在同一个城市,而且很多犯罪分子尽管骗了几百人、几千人,但由于单笔诈骗金额都很小,达不到公安机关的立案标准。此外,犯罪分子在网络诈骗过程中往往使用他人手机卡、银行卡甚至是身份证,这也让公安取证犯难。

以“双11”以后目前最流行的一种网络诈骗——“退款诈骗”为例,骗子会通过一些渠道获取到受害者的网购信息,利用受害者付款后等待收货的时间段冒充卖家,通过打电话的方式联系买家,以支付系统问题等说辞诱导受害者进行退款操作;随后,骗子会给受害者发去钓鱼链接,受害者打开后看到的是高仿电商网页,钓鱼网页乘机诱导受害者输入支付宝账号、密码、银行卡号、身份证号、手机验证码等诸多资料,盗刷用户支付宝和银行卡。

业内人士透露,虽然骗子在整个退款诈骗过程中协同作案,但他们可能在全国不同的地方且相互间也许不认识。所以,仅仅

依靠一两条的报案信息,往往难以获得有价值的线索或证据链,犯罪分子很容易躲避追查。

维护网络安全 仍需多方合力

上海前三个季度有556人在猎网平台举报遭遇网络诈骗,损失总金额近500万元,人均损失高达8084元,比排名第二的重庆市人均损失高出近1700元,在全国各城市中排名居首。《报告》显示:从今年第三季度数据看,网民购买虚拟物品最容易受欺诈,占比为42.9%,其次为手机数码(占26.5%),其中买苹果手机最容易受骗;再次才是网购跑量的最大品类——服装鞋帽(占20.0%)。

“反网络诈骗需要公安、企业和普通网民共同联手。”北京网安总队队长叶漫青承认,伴随网络诈骗案件日益猖獗且各种新型网络诈骗层出不穷,“网骗”已经成为中国用户上网最大的威胁之一。为严厉打击网络诈骗犯罪,今年4月,公安部组织开展打击网络投资诈骗犯罪,打掉了诈骗公司133个,抓获犯罪嫌疑人2000余名;10月30日,国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室部署,自11月1日起开展为期半年的打击治理电信网络新型违法犯罪专项行动。专家指出,共建网上安全生态人人有责。建议网民可多渠道举报恶意程序、恶意网址、诈骗电话、诈骗账户等诈骗信息,还可通过文字、图片、录音、影像等多种方式向平台举报自己被骗的经过。

本报记者 胡晓晶

延伸阅读

挖空心思“白条套现” 当心反被“黑手套牢”

打白条不用还,还能套现?记者今天凌晨在网上搜索关键词“白条套现”,居然跳出来多达576万条纪录。其中,“白条套现+办法”“白条套现+流程”“白条套现+中介”似乎成了输入频率最高的常见提问。对此,京东金融方面承认,作为互联网金融行业的第一款信用支付产品,京东白条在为客户提供“先消费,后付款”的便捷服务的同时,确实也吸引到不少企图套现的诈骗分子,甚至还有不法中介为此“出谋划策”。在京东金融自主研发的“天网”风控系统上,至今累计拦截高风险订单金额已过亿元。

案例1

账号被“撞库” 不法分子趁机套现

被“撞库”后,说不定有人会假借你名义,拼命打白条买买买?家住上海虹桥的王女士近期发现,自己的京东账号突然出现了无法登陆的情况,后来才知道这其实是平台检测到账户异常所做的强制保护。在按提示进行了密码重置等一系列操作后,王女士发现订单交易里莫名其妙出现了多个京东白条交易记录,好在最后均被系统取消交易。经过与京东金融的客服沟通,王女士才知道:原来自己的京东账号被盗取了,不法分子盗号后利用王女士此前已开通的京东白条服务,多次尝试买iPhone 6s。

分析>>>

据乌云漏洞报告平台爆料,已有上亿邮箱数据库被泄露。不法分子会利用互联网已泄露的用户和密码信息,尝试批量登陆其他网站。对此,京东消费金融风险总监程建波建议,为避免个人信息被盗取被“撞库”,不同网站账号和密码最好不要完全相同,也不要再在公共场所点击来历不明的免费WiFi。

案例2

配合中介套现 反被骗走个人信息

令人惊讶的是,在被用户举报的互联网金融安全事件中,个人主动联系并配合中介合伙套现的用户不在少数,然而却更容易“聪明反被聪明误”。在深圳福田上班的李小姐,因为平时喜欢网购,所以京东金融一推出京东白条,她就立即申请开通了这项服务。最近,她注意到多个论坛和社交网络上都出现了京东白条能套现的消息,于是她主动联系了一家所谓的“套现中介”,在提供了自己的京东账户、手机号、银行账号和相关验证码等信息后,坐等收取“好处费”的李小姐却等来了催款通知。原来,当她按“中介”要求用自己的京东白条买了一部iPhone手机、一台佳能相机后,所谓的“中介”就“人间蒸发”了,电话关机、QQ不回,去论坛求助却被人回复:“被骗了!”

分析>>>

本想套现赚点差价,没想到个人信息不仅全都公开示人,而且还不得不“吃”进一堆本来“并不需要”的东西……对此,京东金融方面提醒说,已对相关风控系统不断升级,尤其会对套现、中介代办等风险账户进行预警拦截,并采取账户止付处理。

本报记者 胡晓晶

“双11”当天 全国钓鱼网站攻击频次过亿



“双11”日进千亿元的狂欢已经过去,然而一组网购安全数据却让人不寒而栗。据360互联网安全中心最新公布的数据显示:今年“双11”期间,共为全国用户拦截钓鱼网站攻击1.1亿次。同时,猎网平台当天接到用户报案98起,涉案总金额约118.3万元,人均损失达1.2万元;其中,男性被骗的人均损失几乎是女性的两倍。

大规模钓鱼攻击发生在“双11”前夜,当天仅360互联网安全中心拦截到的钓鱼攻击就有1.8亿次,超过正日子“双11”全天的拦截量。此外,新增钓鱼网站也明显增多,“双11”当天截获到新增虚假购物类钓鱼网站2045个,占全天截获新增钓鱼网站总量的35.7%;其次是假冒银行类钓鱼网站1512个,占比为26.4%。

据悉,最大一波规模攻击出现在“双11”零点抢购开始前的2-6个小时。猎网平台反网络诈骗专家裴智勇指出,“可能有很

多网友在‘双11’狂欢还没开始之前,就已经上当受骗了;再或者就是等到疯狂的抢购之后,才发现自己抢错了地方、误入了仿真的钓鱼网站。”

过了“双11”,网络诈骗又会出现新高峰。最突出的就是“退款诈骗”——以网购交易存在异常或无法发货为由,钓鱼网站通过退款诈骗进行诈骗。据监测,“双11”以后以“淘宝异常订单处理中心”为代表的退款诈骗钓鱼网页,数量即呈现快速增长态势。

本报记者 胡晓晶

