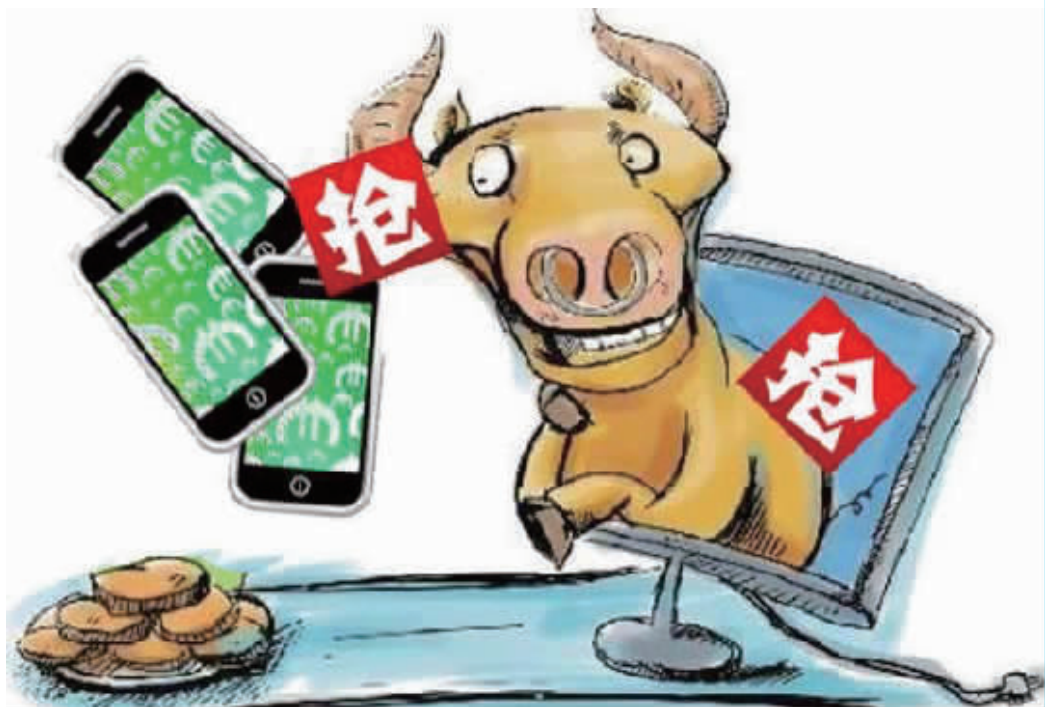


消费者参加网络促销购物多凭运气 “黄牛”团伙开发软件抢购囤货牟利

业内人士揭网络抢购软件神秘面纱

近日,“黑米”抢购软件案在山西省太原市迎泽区人民法院宣判,3名犯罪嫌疑人制作、销售抢购软件构成提供侵入、非法控制计算机信息系统的程序、工具罪被判刑,成为国内首起该领域入刑的案件。

随着互联网技术的发展,一些“黄牛”钻漏洞,针对不同的电商网络平台制作相应的抢购软件,在电商平台推出的秒杀、低价抢购等让利促销活动过程中,通过用非法手段大量抢购,囤积商品,加价转卖牟取暴利。进而导致消费者在面对一些网购平台促销时,拼尽全力却少有机会抢到心仪的低价商品。“黄牛”抢购软件究竟是如何操作的?记者对此进行了调查。



参与网络抢购渠道不少

记者在采访中了解到,目前有不少抢购手机的软件,名称各不相同,记者选取了其中一款下载并安装。

这款软件集预售、抢购、预约、查单、抢购某品牌手机于一身,有这样一些特点:

软件是预付费使用,抢到扣费抢不到不扣费,没有时间限制;不限制登录账号(最多为1000个账号抢购);支持手机登录控制;支持烂单赔偿等。

除了抢购手机,这款软件还可以支持其他电商平台的抢购。以某电商平台为例,目前暂时支持该平台的普通抢购,逐步更新到全面支持抢购。此外,该软件还支持一些购物网站的抢购。

一方面存在抢购软件,另一方面也有专门在网上进行抢购的“黄牛”。

经多方打听,记者以买演唱会门票为由联系上了专门在网上转卖各类门票的王先生。

王先生在其朋友圈中曾发布一条招聘信息:明天就是“双11”,想趁机再招一些人。

记者发现,应聘的人会被拉入一个微信致富群,入群还设置了一个门槛,需要交纳600元入群费。运气好的话,“双11”那天就可以把入群费赚回来。入群后主要从事的工作是研究各个电商平台的减价活动,再通过优惠券或者抢购促销活动低价买入高价卖出的方式赚取差价。

记者在与王先生聊天的过程中了解到,低买高卖的商品来源渠道很多,比如会关注信用卡送电影票的活动,以秒杀的价格买来继而高价转售。除此之外,有的公司在电商平台做促销活动时为了把数据做的好看点会刷交易量,交易成功后返一些钱给顾客,通过购买这类商品再到二手网站转卖也能赚到一笔差价。

消费者受影响难抢购成功

由于抢购软件和“黄牛”增多,消费者在此类商业活动中难以得到什么实惠。

有5年网购经历并经常参加抢购促销活动的田女士说,她几乎每天都要关注某知名电商平台上大牌服饰和护肤品的促销、秒杀活动。一般情况下,在促销活动中,如果网好手快,还是有机会抢购到自己想买的东西。不过,一些优惠力度比较大的秒杀活动基本没有任何机会。

“如果有抢购软件,我们这种只用手机抢购的人连一点机

会都没有。”田女士说。

网络抢购行为不仅出现在一些电商的促销优惠活动中,一些演唱会的门票也有类似现象。

不久前,在北京一家公司工作的范明准备购买自己偶像在南京的演唱会门票。

据介绍,官方售票分两次进行,第一次在购票平台出售200元、400元、600元、800元价位的门票;第二次在微信公众号出售1200元价位门票以及第一次售票过程中查处的少量违规票。

“买票过程异常艰难,基本无法进入购票页面。有时候,好不容易进去了,但无法选票或者无法付款。到最后,所有票全部售罄。随后,网络各大二手票交易市场以及歌手官方微博的评论跟帖中出现大量出票信息,有些人宣称‘各个价位门票均有,如有购买意愿私聊’。在网络售票结束后10天左右的时间里,二手票交易市场出票信息一直很多,价位基本都是票面价翻倍的价格,甚至更高。”范明说。

网络“黄牛”体系化运作

困扰消费者的抢购软件究竟是什么原理?记者采访了阿里云资深安全专家祝建跃。

“网络抢购软件是指针对特定业务(如机票、演唱会门票、抢红包、秒杀促销)编写的自动化程序,模拟正常用户操作(如买票)自动化、批量化的提交请求。因为软件的全自动化特点,其运行速度和大规模并行能力远超过人工,且可以日夜不停地刷票,所以可以在第一时间大量获取余票信息并下单。”祝建跃说。

网络抢购软件又是如何被制造出来的?

“‘黄牛’通过各种渠道如论坛、QQ群、微信群、熟人介

绍等,联系到有能编写抢购软件的技术团队,双方协议好软件的抢购目标和报酬,后者编写好程序后交付前者使用。也有不少技术型的黑灰产团队提供现成的针对知名业务编写好的软件进行售卖。现在,不少专业‘黄牛’团伙自身就具备相当强的技术团队,从研发到销售一条龙,已经是非常有体系的团体化运作。”祝建跃说。

在票务领域,网络抢购尤为突出。

“购票的渠道越来越丰富,从网页到App、微信公众号、各类H5,再到第三方渠道的API,‘黄牛’只需要选择防护最薄弱的一环即可达到目

的。现在的‘黄牛’团伙专业程度非常高,甚至可以与专业的安全公司正面抗衡,双方在攻防技术上不断进行对抗和博弈,永无休止,不存在一劳永逸的解决方案。很多‘黄牛’团伙有专门的资源,可轻易购买到真实手机卡,完全模拟正常用户的行为。对此,票务方难以辨识。随着智能手机、物联网设备的普及和安全漏洞的频繁爆发,‘黄牛’手上掌握的‘肉鸡’资源动辄几万,传统的基于IP频率之类的防护手段应对海量低频的模拟请求已经捉襟见肘。”祝建跃说。

(据《法制日报》)