

虚构原价、捆绑销售、集赞骗局 “双十一”这些坑你掉过吗？

全网最低价比原价还贵、集赞优惠竟是骗局……一年一度的“双十一”促销盛会如约将至,各大电商平台强势宣传“烧脑”促销规则,琳琅满目的商品都被贴上优惠折扣的标签。然而,“低价风暴”背后,有哪些套路? 隐藏哪些陷阱?

“低价风暴”有猫腻:虚构原价、捆绑销售、集赞骗局

四川消费者杨女士在某购物平台网店“原创设计服装店”关注了一件标价为559元的连衣裙多日,准备网店搞优惠活动时再买。“双十一”之前,网店宣传全场包邮、满500减20元,杨女士当机立断下单付款539元购买了心仪的连衣裙。

三天后,杨女士又上该网店选购外套,却发现之前下单购买的连衣裙标价只要335元,居然又大幅度降了204元! 杨女士要求网店退还差价,网店却拒绝退钱……

“双十一”前夕,类似虚构原价现象屡见不鲜,捆绑销售也是常见套路。

最近,市民胡女士在某网络平台购买了一张火车票,票价为65元。但要额外收取两张优惠券费用共30元,网站显示,优惠券可享受7*24小时预订服务、

商家套路深:虚假宣传、先涨后降、“钓鱼”陷阱

记者了解到,随着“双十一”来临,商家的套路主要表现在虚假宣传、先涨后降、“钓鱼”陷阱等方面。

——虚假宣传误导。四川省律协消费者权益保护专业委员会副秘书长单静说,一些不良商家为了在“双十一”期间刷销量,会用一些虚假词汇来做宣传,趁机误导消费者,比如,“产量一直领先”“全网最低价”等,背后大多是虚构的事实和隐藏的真相。

北京安博(成都)律师事务所律师韦海军说,虽然法律有欺诈增加三倍赔偿的规定,但不少商品销售者存侥幸心理,认为不被抓到就不会被罚款,因此,虚假宣传反而成为一种常见的商家销售套路。

——利用信息不对称先涨价后打折。“一些商家通过这种方式诱骗消费者消费,侵犯了消费者的知情权和选择权。”泰和泰律师事务所律师廖华说。

“我看准要买一款婴儿车,

消费者擦亮眼学会较真 行业强化自律和社会共治

廖华说,从消费观念上,消费者一定要学会较真,要敢于依靠相关组织,依靠专业人士,拿起法律武器维护自己的合法权益。

单静等专家认为,在遭遇“钓鱼式”购物陷阱时,若商家以不正当理由拒绝兑现,消费者可以向当地市场监督管理部门投诉商家的虚假销售行为;也可向当地保护消费者权益组织请求调解;还可向人民法院提起诉讼。

记者了解到,根据消费者权益保护法的规定,经营者提供商品或者服务有欺诈行为的,应当按照消费者的要求增加赔偿其受到的损失,增加赔偿的金额为

客服服务、快速退改签服务、短信提醒服务等,并且不能取消,胡女士支付了30元优惠券费用,但事后发现,这些优惠服务根本是“纸上谈兵”,没有一项能实现,但钱又退不了。

“不仅没买到便宜,反而还白交了钱。”胡女士后悔地说。

微信集赞低价购物骗局也是“双十一”来临前朋友圈的刷屏套路。

“只要将活动内容分享到朋友圈,并累计点赞28个,就可以低价领取生蚝”——家住四川泸州的易女士被这句广告词吸引,急忙在朋友圈吆喝求点赞,在活动期间完成集赞数量后,支付了49.6元购买了10斤生蚝。但在约定提货时间去领取生蚝时,商家却说活动太火爆,生蚝已领完了……

上个月原价还是1300元,最近几天突然变成了2400元,还写着‘双十一’将大降价500元,实际上比原价贵多了……”市民杨先生说。

——“钓鱼式”低价陷阱。记者了解到,在一些网上购物平台、微信平台上,类似通过免费集赞、免费转发、免费试用等噱头来诱导消费者下单,有的故意不事先写明押金定金是否退还,有的将“参加该活动一律不能退款”等条款模糊处理写在活动页面最后,造成消费者钱物两失的情况不在少数。

四川博绅律师事务所律师李清说,消费者参与了这些“钓鱼式”低价购物活动,后期商家就会以“货物发完了”“订单未使用”等借口,拒绝退还收取的押金,或者告知退款要收取高额手续费,甚至实际提供的商品或服务与宣传不符,来坑骗消费者。有的微信集赞还需要提供身份信息和社交账号,很可能导致个人信息被盗。

消费者购买商品的价款费用的三倍。

北京盈科(成都)律师事务所律师高涛说,“双十一”来临,网络平台侵害消费者合法权益的行为时有发生。建议广大消费者尽量选择正规大型的网购平台,下单前仔细阅读相关条款,了解所购商品或服务的使用规则和限制性条款。注意保留证据,如下单付款凭证、商品宣传信息及聊天截图等,以便发生纠纷及时有效维权。

相关专家也指出,针对“双十一”种种购物陷阱,还需要加强监管和社会共治。(据新华社)

收集主体多、安全保障弱、亟需强立法—— 谁来保护我们的生物特征信息？

近日,杭州野生动物园规定,不录入人脸信息将影响该公园年卡的正常使用,引起社会关注。

当前,公民的指纹、面部特征等生物特征信息是否面临被过度采集的风险? 哪些主体正在获取我们的生物特征信息? 相关信息保护在哪些方面亟需补强? 新华社记者就此展开调查。

公众生物特征信息 屡遭过度收集

记者从北京大学法学院副院长薛军教授处了解到,当前,人脸、指纹等个人生物特征信息已经成为身份证号码、手机号码等信息之外,过度搜集公民信息案件中新的“重灾区”。

同时,由于生物特征信息与个人财产、人格权益之间的联系日趋紧密,信息一旦丢失或失控,将给信息所有者造成巨大且难以挽回的损失。

这并非杞人忧天。2019年2月深圳某人脸识别企业被证实发生数据泄露事件,超过250万人的核心数据可被获取,680万条记录泄露,其中包括身份证信息、人脸识别图像及GPS位置记录等。

一些软件也涉嫌过度采集用户的生物特征信息。此前,中国消费者协会曾发布《100款App个人信息收集与隐私政策测评报告》。报告显示测评的100款App中,10款App涉嫌过度收集个人生物特征信息。一度成为互联网热门应用的某换脸软件开发企业,也在今年9月因涉嫌未依法依规收集使用用户个人信息被工信部约谈。

有国内知名互联网企业视频识别安全专家向记者透露,当前存在为数不少的不法分子、数据黑灰产从业者通过通过真人认证,达到注册虚假账号或者直接侵犯他人账号的目的,需要相应的人脸信息,甚至在国内已催生出一一定规模的“过脸产业”。

记者搜索互联网,发现网络论坛中存在大量针对电商平台、特定设备的“过脸”技术解答,甚至有完整“过脸”技术教程,包括软件选择、脚本设置等。一些网站上还有“过脸软件”代码链接,随意供人下载。

我们的生物特征信息流入何处? 是否安全?

那么在日常生活中,究竟是谁热衷于记录和储存我们的生物特征信息呢? 奇安信网络安全研究中心主任裴智勇告诉记者,当前大致有三类主体。

首先是部分视频监控的运营主体。比如通过商场酒店、会议场馆等公共场所视频设备采集信息。

其次是一些公共职能部门、大型互联网企业、商业机构等,经过用户授权,采集包含用户个人生物特征的数据信息。

第三是科研机构因为科研需要收集使用,如存储一定规模的样本供人工智能进行学习、训练。

浙江大学计算机学院人工智能研究所教授李玺表示,目前公民生物特征信息的主要采集储存主体提供信息安全保护的能力水平参差不齐,信息公开透明度也不够,容易导致海量信息面临安全风险。

与此同时,业内人士透露,目前在授权采集过程中,大量商业主体为降低自身成本,通过格式条款或单方告知的形式“逼”处于弱势地位的公众出让生物特征信息,甚至在合同约定中暗含自我免责条款。这些都不利于相关信息保护。

“未来也不排除根据收集来的数据重建个人生物识别特征的可能,比如3D打印技术‘复刻’人脸。到那时我们所面临的风险就不仅仅是虚拟世界被入侵,而是现实生活中被冒充。”奇安信集团副总裁左英男说。

正、邪技术力量仍将缠斗 法律空白亟需填补

受访网络安全专家认为,人脸、指纹、虹膜甚至基因,生物特征信息因其随身性、唯一性,将被愈加广泛地应用于金融、购物、安全等生活场景的趋势不可逆转。但其可复制性则同样决定了围绕信息安全技术所展开的“道魔之争”将长期持续。

记者了解到,目前针对“换脸”潜在的风险,技术层面主要可以通过“活体检测+人脸比对识别”应对,同时通过翻拍、3D结构光、多维度生物特征信息等辅助技术,也能够一定程度上增加相关技术的安全性。

有专家认为,当前相关法律法规规范层面的缺位同样亟需填补。

据浙江浙杭律师事务所高级合伙人姜海斌律师介绍,我国网络安全法规定了“谁收集、谁负责”的原则,并规定收集个人信息须经被收集者同意,其中包括个人生物特征信息。但对于收集相关信息主体需要提供何种程度的保护力量、如何评估与公开、公民个人敏感信息的保护层级、具体保护措施等关键问题,目前均尚未制定具强制力的法律规范。

2018年5月,全国信息安全标准化技术委员会颁布实施《信息安全技术个人信息安全规范》,作为推荐性国家标准,其中将生物识别信息等明确归为“一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等”的个人敏感信息。

北京航空航天大学法学院院长龙卫球认为,该标准针对个人信息收集、保存、使用、委托处理等环节提出要求,落地网络安全法的原则性规定,填补国内个人信息保护在实践标准上的空白,为企业进行个人信息保护合规提供具体指引。(据新华社)