电商和O2O行业诈骗那些事儿（下）——安全小课堂第九期

2016-05-06 京东安全应急响应中心

安全小课堂第九期

本期，我们接着和小伙伴——唯品会高级安全研究员森尼、大众点评业务安全负责人纪东、携程高级安全研究员小胖胖聊聊电商和O2O行业诈骗那些事儿~

1

豌豆妹

请问如何防范电商和O2O刷单情况的出现呢？

小丸子

从c端b端两侧进行考虑。c端对用户的注册、登录、下单、支付等事件进行风控扫描和异常拦截。对b端识别作弊聚集的商家、商品，识别虚假商户。大额的优惠建议仅限app，可以利用设备信息。

小新

1、针对单账户的恶意识别，包括行为和维度数据；2、针对行为点的恶意控制，包括业务控制，和恶意防护过滤；3、针对事后的数据分析以及业务反馈，进行离线拦截，同时数据反推到1和2，进行事件闭环。同时自身数据外，还可以结合外部数据，包括一些大公司的服务和行业黑数据进行综合应用。

葫芦娃

我们会从注册，登录，下单过程结合ip，手机号，用户行为等多维度判断是否为恶意用户，通过安全大数据系统进行关联分析判断用户是否在刷单，针对刷单用户会有下单拦截，取消，甚至冻结账号等措施。包括security@ctrip.com也提供相关恶意接口服务。

风险库

根据不同层面的恶意行为计算风险值，多年沉淀，千万级别手机号码库，帮助企业有效防御羊毛党。

哆啦A梦

针对活动的防刷，我们在上线前会做安全评审，根据不同的活动类型给出不同的防刷策略，比如短信，用户ip等等维度。活动上线后会进行安全监控，同时会分析异常刷单的用户，进行相应的处置。

2

豌豆妹

如何有效地监测刷单异常？

小新

1、下单维度数据聚合；2、用户手机号，地址信息异常匹配（比如某些高危区域）；3、分类订单异常监控，比如某个价格订单或者某类商品订单突增；4、维度数据的层级关联，如一个人订了一个外卖，可能这个人也是一个送货员，进行多层级数据关联，可以看到更广的信息。

3

豌豆妹

能聊聊乙方风控平台的优势以及共享黑数据的调用么？

小丸子 

乙方在某些领域的数据会更加的专业，比如代理ip的精准检测等，我们可以通过他们的接口进行查询，把结果作为用户信用的评判因素之一，加入到风控系统进行评分。

葫芦娃 

同意。乙方的优势在于对接了多个平台，平台之间的黑名单数据可以共享。但是乙方提供的黑名单也不能直接使用，准确率较难保证，而且不稳定，只能用于聚合类的策略。

哆啦A梦 

共享黑数据是建立生态圈比较好的方式，当然要互信互利，同时自身业务应用也需要对数据进行一定的把控 ，数据是否能起到很大的效果或者数据质量的保证需要进行大量的实践。

豌豆妹

三人行必有我师。感谢三位小伙伴和核心白帽子陪伴我们聊聊电商和O2O行业诈骗那些事儿~大家如有感兴趣的话题也可发至JSRC官方微信公共号，让我们共同畅游在知识的海洋里~下期见哟~🖤🖤🖤




安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们