

聊聊金融反欺诈那些事儿—安全小课堂第三十四期

原创：京东安全应急 京东安全应急响应中心 2016-11-18

安全小课堂第三十四期

近些年互联网金融发展迅猛，出现很多理财平台、支付渠道、信贷平台，但是大部分平台的风控做得一般。网络安全事故越来越多，平台的信息泄漏太严重，导致出现各种金融诈骗事件，比如盗卡、盗号、线下盗刷、伪冒申请注册等。现在的电信诈骗，愈发严重。为了更好地保障用户的权益，金融反欺诈就应运而生。本期，我们来聊一聊金融反欺诈那些事儿~

本期我们邀请到
银客集团安全专家5nds1t
邦盛的安全专家鲍鲍
大家欢呼
ヾ(*°▽°*)ノ

/ 01 /



豌豆妹

能介绍下金融反欺诈的背景么？



小新

近些年互联网金融发展迅猛，出现很多理财平台、支付渠道、信贷平台，但是大部分

平台的风控做得一般。网络安全事故越来越多，平台的信息泄漏太严重，导致出现各种金融诈骗事件，比如盗卡、盗号、线下盗刷、伪冒申请注册等。现在的电信诈骗，愈发严重。为了更好地保障用户的权益，金融反欺诈就应运而生。

平台的安全性存在问题，个人数据严重泄漏。信息泄露导致的信息买卖，是促发风险的首要条件。另外，因为盗卡的案件，银行不负责赔付，需要渠道承担，这倒逼着各家金融公司开始做反欺诈。

目前中国互联网的金融反欺诈，还在各自防止资损阶段，反欺诈的核心是保障平台各家不用赔钱或被央行处罚。

/ 02 /



豌豆妹

能说说金融反欺诈的重要性么？



哆啦A梦

金融业务中包含大量的用户真实身份信息和资金交易，做好反欺诈工作能保障这些重要信息不泄露。除此之外，反欺诈工作能保证公司进行推广，发放福利时，不被薅羊毛，保证推广活动的效果，且信贷、借贷等业务若发生欺诈事件会造成直接的经济损失。由此可见，反欺诈工作非常重要。



葫芦娃

简单说一下，目前中国从事互联网黑产的人员超过100万，大陆公民个人身份证公民信息泄露超过70%，只是黑色产业哦~比如虚假交易、专业的薅羊毛、套现、信息爬取、木马流量商等，不包括灰色产业。现在情况下，不做反欺诈，就得赔钱，很实际的问题。

/ 03 /



豌豆妹

反欺诈系统中常用到的相关技术有哪些？目前来说，最有效的技术有哪些呢？



小丸子

设备指纹，这个界内通用的吧。现在市面上的数据太多了，各有千秋。不讨论数据覆盖面的情况下，代理ip识别、图形验证码、用人机识别技术、基站定位，也可以识别虚拟机。



小新

数据关联分析，后面的核心风控模型。我们从近亿条数据中分析用户行为，对用户进行画像，同时借助第三方借贷、交易、征信等数据，区分可信用用户和存疑用户，业务上建立风控模型，根据不同情况调整风控策略。反欺诈系统需要针对不同业务建立不同的风控模型，并收集不同渠道的第三方数据进行综合数据分析，所以我们现在使用的都是自研的风控系统。



豌豆妹

方便详细说说自研的风控系统么？



柴可夫斯基

自研的风控系统就是考虑公司自身情况，由我们自己开发的风控系统，反欺诈我们通

常会考虑技术和业务等方面，分为实时系统和离线系统，实时系统是风控系统的核心。

实时系统有风控评分系统、旁路的安全审计系统。对于不同业务，实时系统对延迟性要求是不同。比如信贷业务，不需要实时放款，中间的实时性要求就不是很高，有几分钟的缓冲时间。通过旁路的安全审计，计算当前用户是否存在攻击行为，或者当前设备，ip是否有过类似的不符合模型的行为都会影响后面的评分。

/ 04 /



豌豆妹

那金融反欺诈在技术和业务方面分别如何实施呢？



葫芦娃

业务待技术架构实施完，补充数据和业务策略。想办法收集尽可能多的数据（如多家共享数据）。然后就是各种数据的埋点、分析数据、调整策略等。



豌豆妹

在金融反诈骗的技术实施过程中，是否可以应用机器学习？



哆啦A梦

有数据就可以，但是不会完全采用机器学习，还是需要人为的干预和审计，再分析调整策略。策略不是一簇而就的，可能需要几年时间。



微信公众号：jsrc_team

新浪官方微博：

京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂