QCon

全球软件开发大会【上海站】

无“诈”不欢的互联网业务

锦佰安　冯继强

极客时间

重拾极客精神·提升技术认知

每天10分钟，邀请顶级技术专家，为你传道授业解惑。

扫一扫，试读专栏

主办方 Geekbang 极客邦科技 InfoQ

ArchSummit

全球架构师峰会 2017

12月8-9日 北京 · 国际会议中心

AiCon

全球人工智能技术大会 2018

助力人工智能落地

2018.1.13 - 1.14　北京国际会议中心

扫描关注大会官网

APSEC 2017

南京大学 NANJING UNIVERSITY × Geekbang 极客邦科技 | InfoQ

冯继强（网名：风宁）

国内知名网络安全专家。
现任锦佰安信息技术有限公司创始人&CEO。
目前创业，主导公司产品研发负责行为识别认证产品；设计研发及移动互联网、物联网身份管理，帐号安全解决方案。
曾担任通付盾首席安全官、青藤云首席安全官、智泰华瑞副总裁，担任多个政府部门及大型企业网络安全顾问。
SACC中国架构师大会顾问组专家成员、Kcon黑客入门闭门讲师、Xkongfu演讲嘉宾。

CONTENT目录

PART1

何为互联网业务欺诈?

何为互联网业务欺诈?

- 业务风险
- 资金风险
- 品牌负面风险

互联网业务欺诈特点

专业化

投入专业设备，购买大量的廉价智能手机用于注册账户，购买大量小额手机卡，通过猫池和自动化管理软件成功实现短信批量接收验证码的功能。

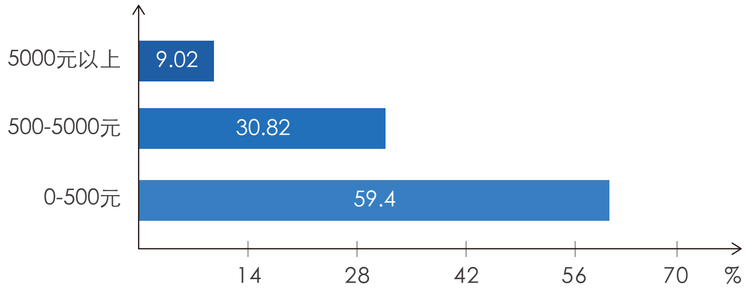
团伙化

流程越来越严谨，分工越来越细致，团伙化工作，经常互换身份，辨识难度越来越大。

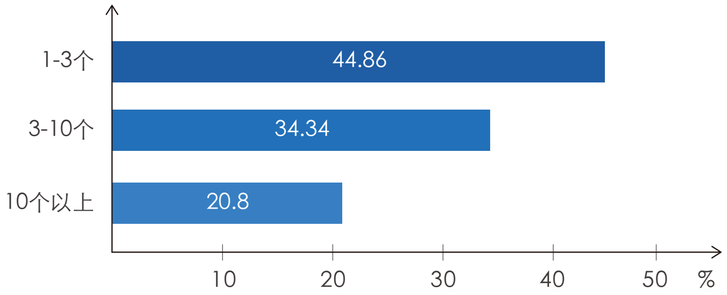
地域化

规模越来越大之后，需要大量可靠的团伙成员和合伙人，为了可靠起见经常寻找同乡入伙，在地方扎堆集中作案的情况越来越多。

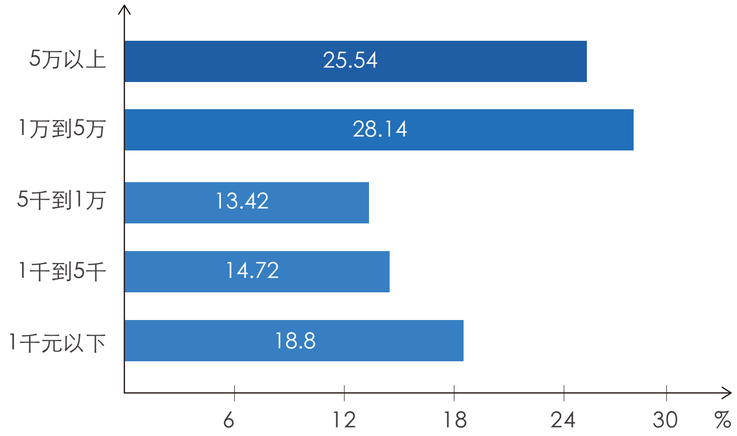
欺诈业务冰山一角：羊毛党



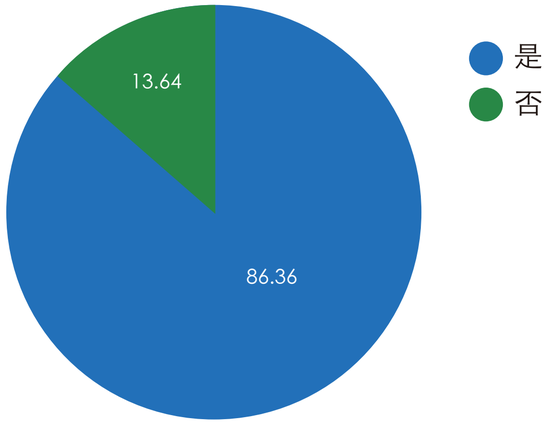
薅过羊毛的平台数量



薅羊毛的收益



用于薅羊毛的本金



薅羊毛是否踩过雷

互联网业务欺诈常用技术

设备伪造
身份伪造
行为特征伪造
手机号
银行卡号，CVV，金融账户

模拟器/刷机
某些备案网拿到的身份证/人才市场
软件自动全页面下载，接入打码平台
常见猫池养号及收码平台
钓鱼获取银行卡号/支付宝号

互联网业务欺诈冰山一角

百度大量充斥王者金币贩售信息

某宝天猫店铺大量贩售挂机金币

PART2

后台业务数据只是假象

后台业务数据只是假象

业务欺诈数据刷量业务盛行

知乎 首页 发现 话题 搜索你感兴趣的内容...

网络营销 应用程序 (Application Programme) 运营推广

那些刷App下载量的营销公司怎么实现一天刷量几万次的？用的什么工具啊?

正文

315揭秘 | 数据曝光微信刷量黑幕 (2016-03-15 19:30:35)

10万下载量刷入iOS免费TOP10，APP被苹果处罚降权！

发布者: 鸟哥笔记-馒头 来自: APP营 2014-12-12 16:20

网易首页 > 新闻中心 > 新闻 > 正文

明码标价，刷分刷流量刷口碑

2017-02-22 01:59:56 来源: 北京日报(北京)

各种黑幕刷量交易明码标价

欺诈数据刷量都有谁

新媒体运营人员

为了完成KPI，向老板
和投资人交差

乙方公司

为完成运营效果指标
忽悠甲方公司

层级代理商

为完成销售指标
忽悠上级厂商

微信自媒体

通过营造“微信大号”
形象，赢得广告利益

到底损失有多大

一万个虚假用户，自然流量70元一个，预算70万

CASE1

如果渠道给你全部上假量，比如说是墙量，他的成本大概是2.5元一个，那么您的显性损失成本可以计算为：（70-2.5）*1万=67.5万。

CASE2

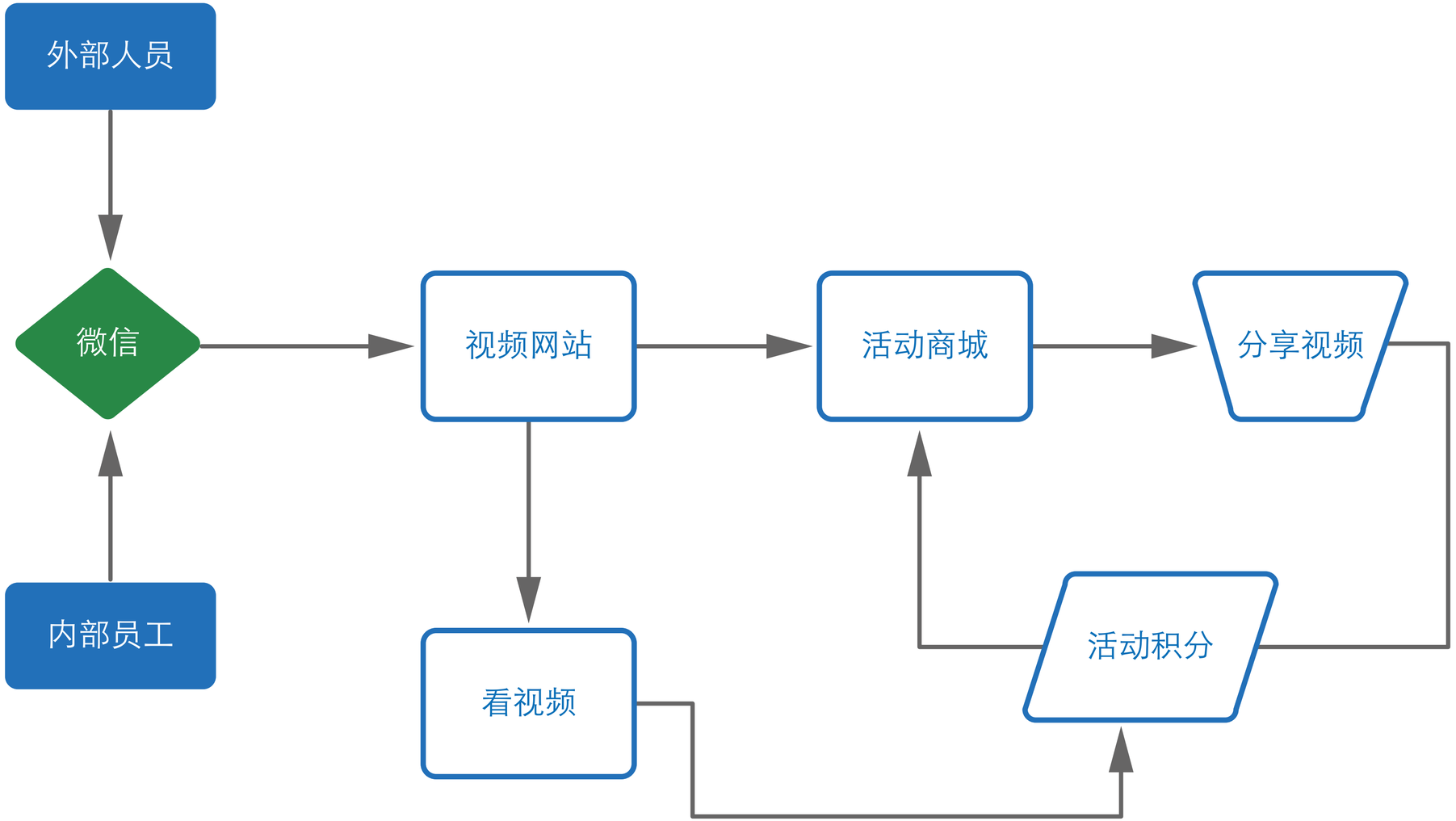
如果对方给你上的是机刷量，他的成本大概是0.5元，那么您的显性损失是69.5万。

如果对方是按照比例掺的各种假量，请遵照上述公式，计算出显性的损失成本。

PART3

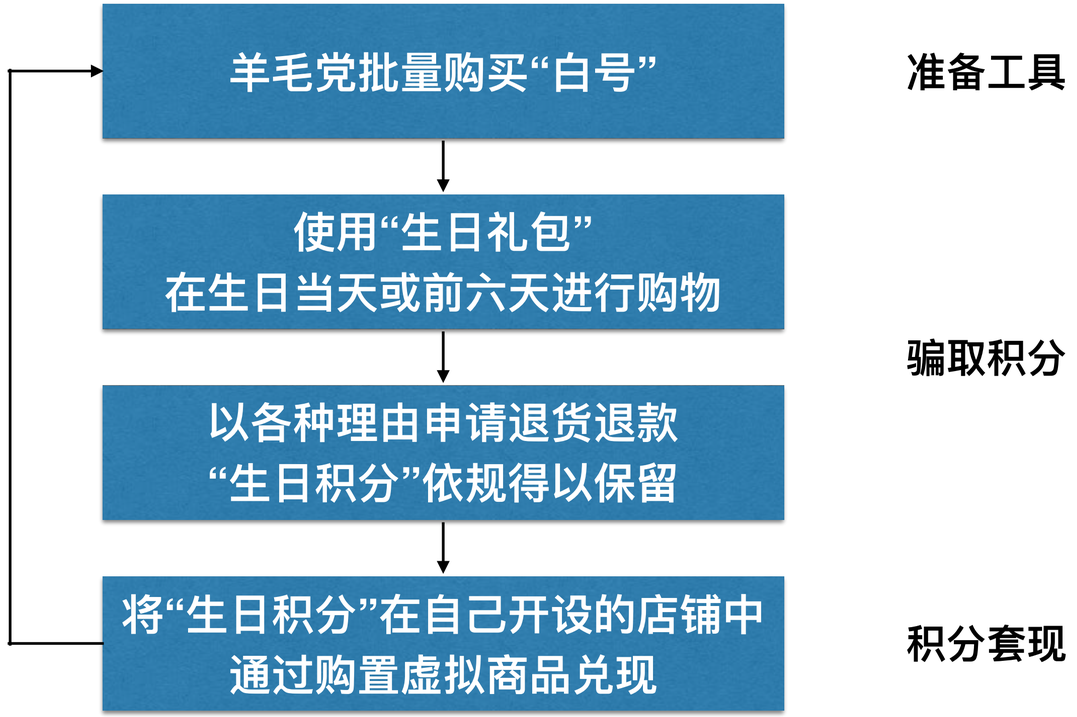
真实业务欺诈案例复盘

真实业务欺诈案例复盘



真实业务欺诈案例复盘

天猫生日礼包双倍积分



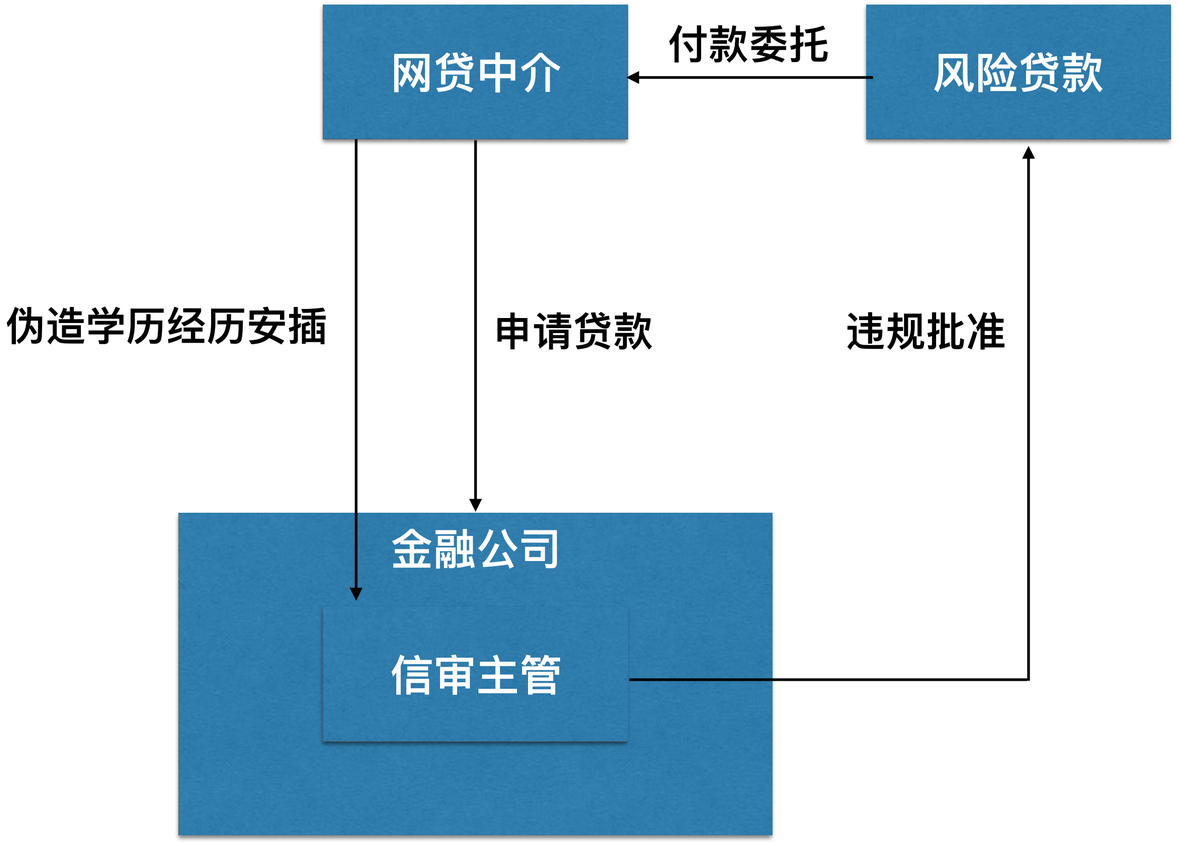
“只能说他们钻了天猫积分规则的漏洞，是在规则允许下的交易。”

——卢伟律师表示将对此案进行无罪辩护

真实业务欺诈案例复盘

中介去消费金融公司卧底，一场关于金钱和欲望的“无间道”| 一本特写

原创 2017-06-20 一本财经 一本财经



中介利用卧底渗透金融公司流程

PART4

业务情报实现精准风控

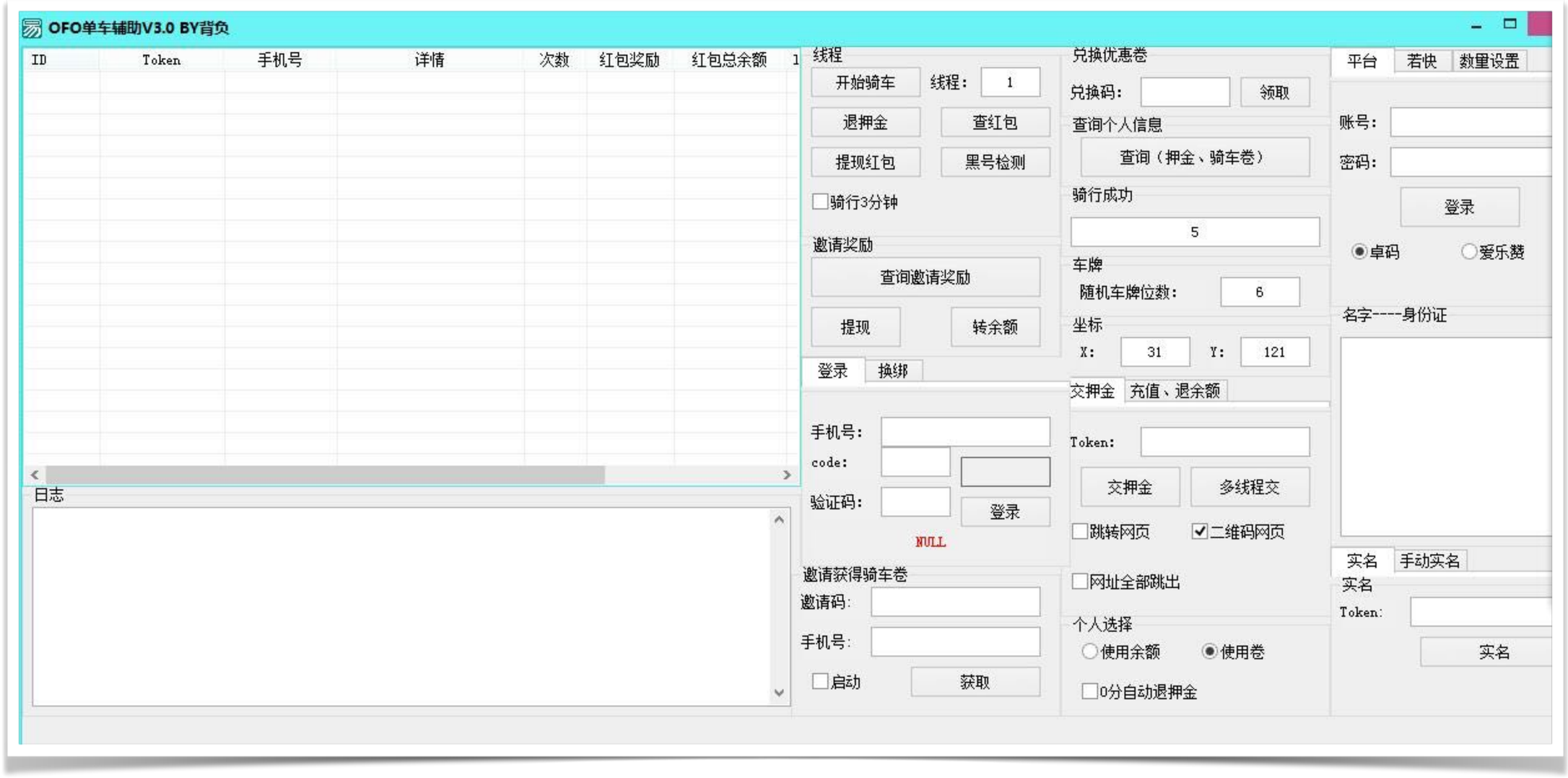
业务情报实现精准风控


OFO单车红包小助手 员工版
ID
phoen
status
余额
已提现
卷数
次数
267 13794336474 有优惠卷,该号未交押金. 6.28 0 1 0
268 13537516414 有优惠卷,该号未交押金. 0 59.3 11 0
269 15817467516 有优惠卷,该号未交押金. 0 33.22 11 0
270 15818597160 有优惠卷,该号未交押金. 0 45.28 11 0
271 15914047202 有优惠卷,该号未交押金. 0 58.17 11 0
272 15818596674 有优惠卷,该号未交押金. 0 37.29 6 0
273 13682430876 有优惠卷,该号未交押金. 0 33.47 11 0
274 13641458547 有优惠卷,该号未交押金. 0 43.67 11 0
275 15814008648 有优惠卷,该号未交押金. 0 46.45 6 0
276 13682430437 有优惠卷,该号未交押金. 0 0 11 0
277 15814642949 有优惠卷,该号未交押金. 0.03 0 11 0
278 15012743415 有优惠卷,该号未交押金. 0 37.76 6 0
279 13714437432 有优惠卷,该号未交押金. 0 41.72 11 0
280 15914032656 有优惠卷,该号未交押金. 0.03 0 11 0
281 13537516373 有优惠卷,该号未交押金. 0 35.61 6 0
282 15012739456 有优惠卷,该号未交押金. 0 0 11 0
283 15012743835 有优惠卷,该号未交押金. 0.03 0 11 0
接码平台
打码平台
平台选择: 玉米平台
接码帐号: 20828-cng
接码密码: ******
宽带名称: 宽带连接
宽带账号: 无需填写
宽带密码: ****
验证间隔: 10000 更换IP地址
自动拨号
延迟: 15
线程数: 10 100000
一键支付
停止
做号
提现红包
2017年5月8日21时31分30秒==>>OFO小助手启动成功...

业务情报实现精准风控


ID
Token
手机号
详情
骑车次数
红包奖励
红包总余额
线程
开始骑车
线程：
1
退押金
查红包
提现红包
结束行程
登录
手机号：
code：
验证码：
登录
NULL
换绑
Token：
手机号：
验证码：
换绑
NULL
走邀请获得骑车卷
邀请码：
手机号：
邀请
兑换优惠卷
兑换码：
领取
设置成功骑行次数
5
查询个人信息
查询（押金、骑车卷）
实名
Token：
姓名：
身份证：
实名

业务情报实现精准风控


OFO单车辅助V3.0 BY背负
ID
Token
手机号
详情
次数
红包奖励
红包总余额
线程
开始骑车
线程：
1
退押金
查红包
提现红包
黑号检测
骑行3分钟
邀请奖励
查询邀请奖励
提现
转余额
登录
换绑
手机号：
code：
验证码：
登录
NULL
邀请获得骑车卷
邀请码：
手机号：
启动
获取
日志
兑换优惠卷
兑换码：
领取
查询个人信息
查询（押金、骑车卷）
骑行成功
5
车牌
随机车牌位数：
6
坐标
X：
31
Y：
121
交押金
充值、退余额
Token：
交押金
多线程交
跳转网页
二维码网页
网址全部跳出
个人选择
使用余额
使用卷
0分自动退押金
平台
若快
数量设置
账号：
密码：
登录
卓码
爱乐赞
名字----身份证
实名
手动实名
实名
Token：
实名

互联网业务反欺诈技术

IP/账号识别与限制

图片验证码+短信/语音验证码

通用设备识别技术

+

设备指纹
（设备识别）

行为识别
（机器人识别）

数据服务
（实名稽核+数据风险评估）

风险管理平台
（风险决策）

互联网业务反欺诈技术

人

1、是真实的个人信息还是盗用 / 伪冒的信息

2、是人在浏览网页还是机器操作

3、是否是高风险的用户

设备

1、是真实的物理设备还是虚拟机/模拟器

2、是否是常用的设备

3、是否是伪造的设备

4、设备是否是高风险设备

账号

1、是真实的账号还是“小号”

2、账号是否泄露

3、账号是否被盗用

行为

1、是真实的交易还是虚假的交易

2、是否是合法的交易

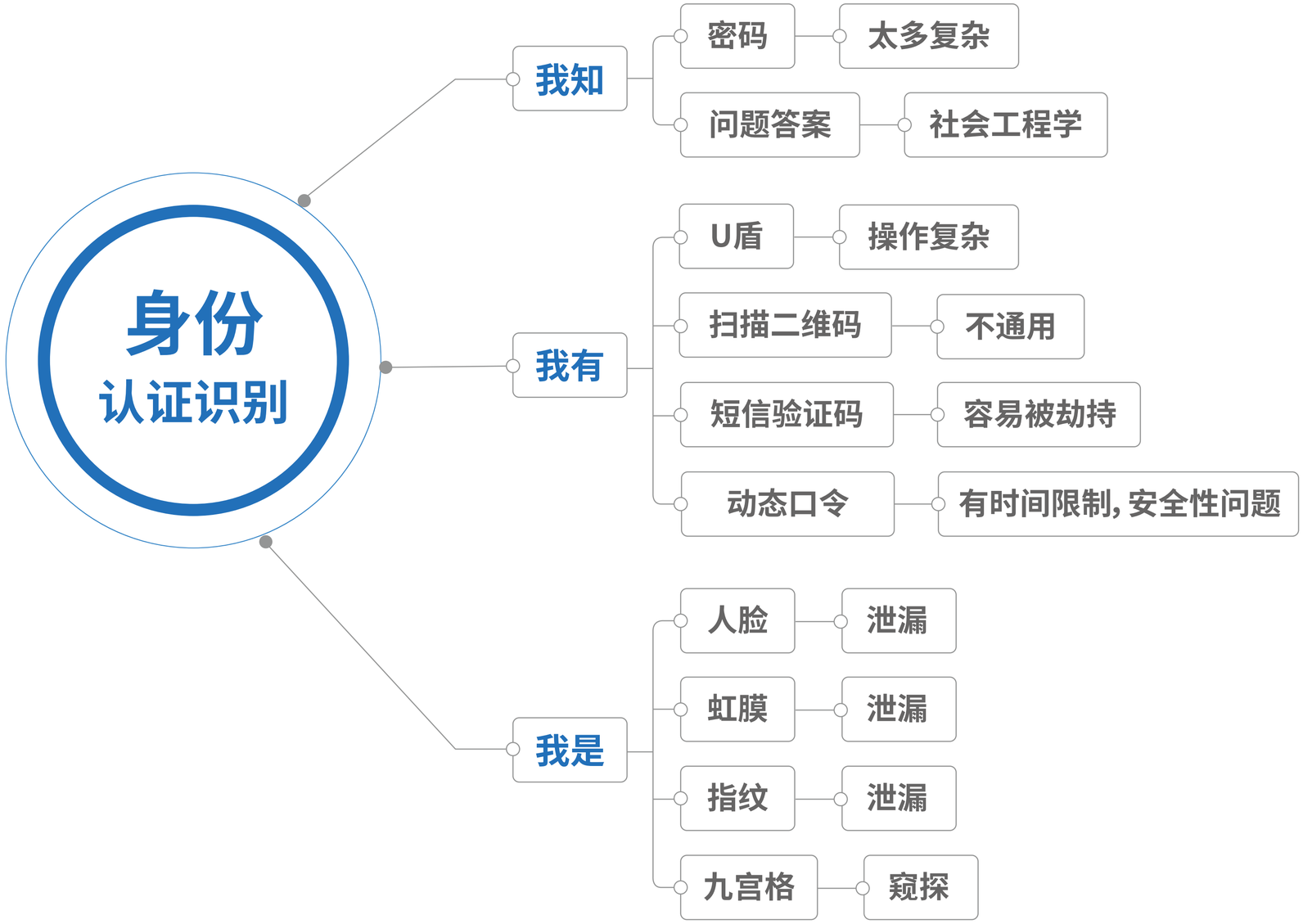
3、是否是真实的评价

4、是否存在隐含的关系

PART5

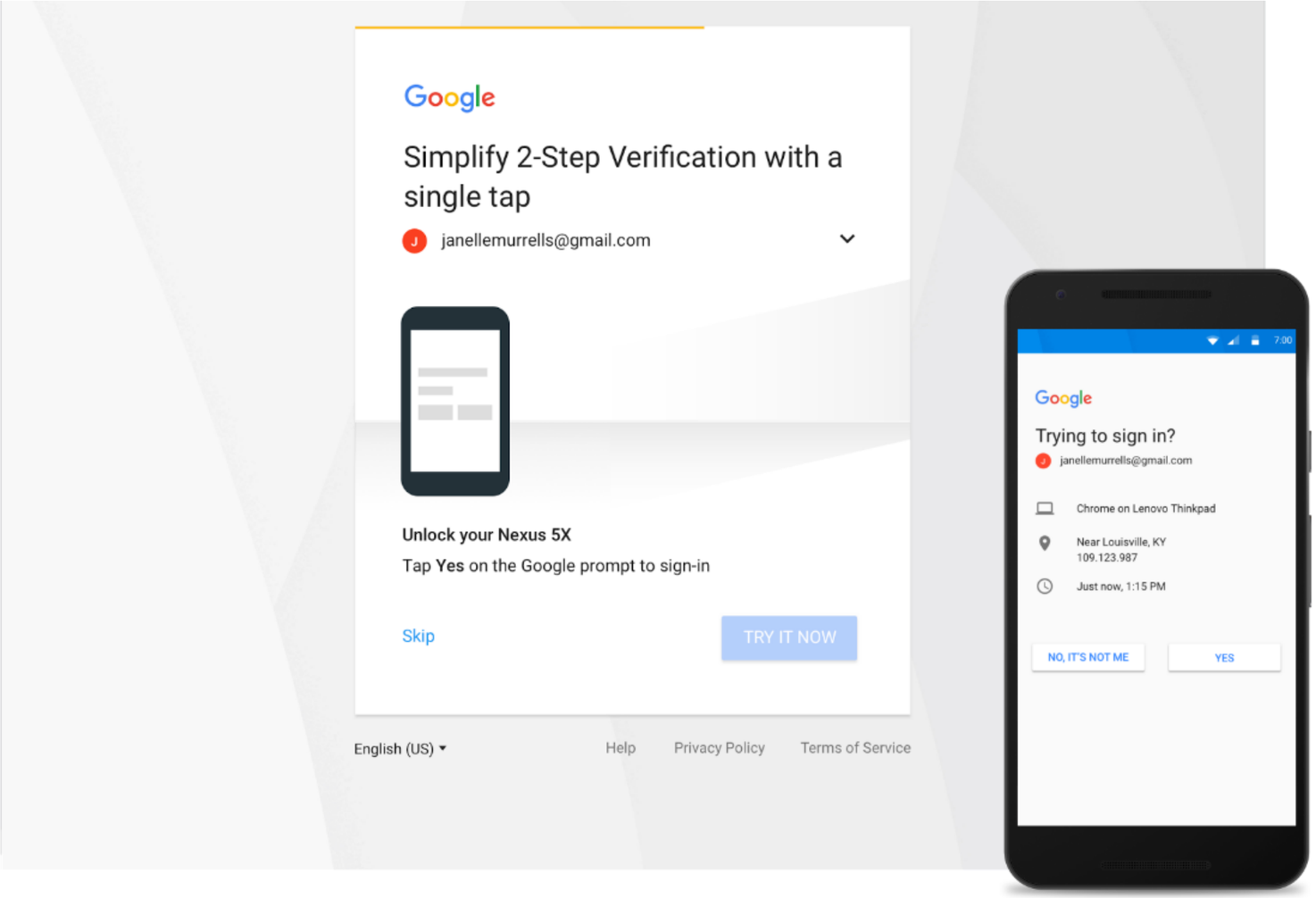
传统身份认证的安全隐患

传统身份认证的安全隐患



短信验证码存在重大缺陷

Google 二步认证方案将用手机提示取代短信验证码



验证码面临的问题：

1.伪基站劫持

2.Wi-Fi钓鱼劫持

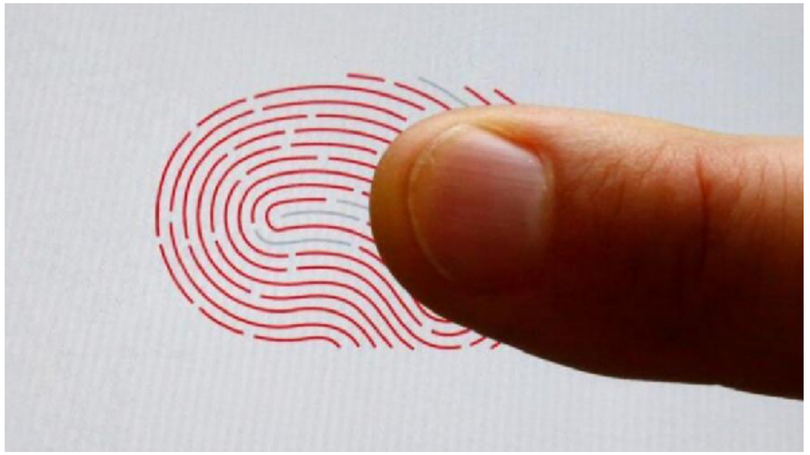
2.手机木马病毒劫持

3.广播模式下复制卡同步接收

……

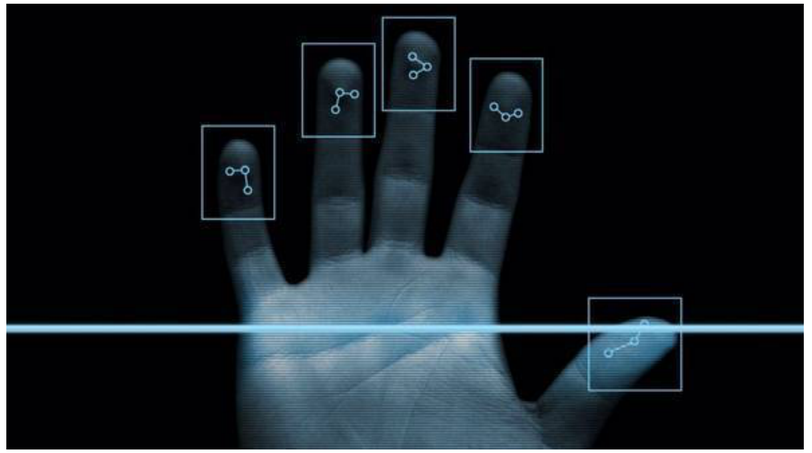
指纹识别存在重大缺陷

人体生物密码具有唯一性和不可变更性，一旦泄露就是终身泄漏



指纹识别缺陷一：不安全

纽约大学和密歇根州立大学的研究人员对指纹识别安全性提出疑问，他们使用人工物理指纹的制造技术开发的“万能指纹”解锁成功率高达65%。



指纹识别缺陷二：可复制 / 易操控

指纹容易被复制，或当人处于无意识状态时，别人可以操控你的手指。例如，可以通过V字手势照片里提取指纹，然后通过3D打印硅胶指纹套。

人脸识别存在重大缺陷

人体生物密码具有唯一性和不可变更性，一旦泄露就是终身泄漏

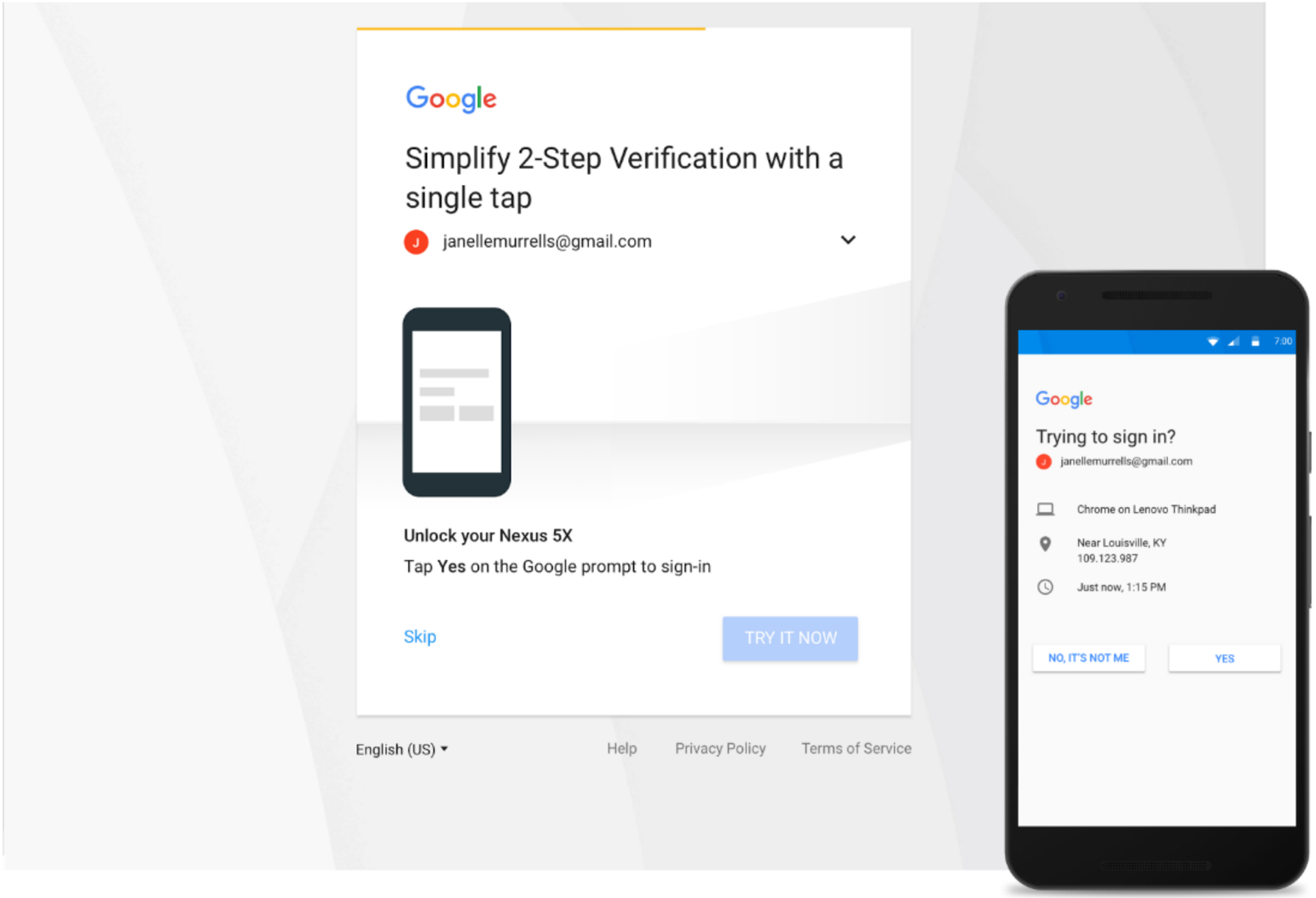
人脸识别缺陷一：相似性

人脸识别缺陷二：不稳定性

人脸识别缺陷三：可复制性

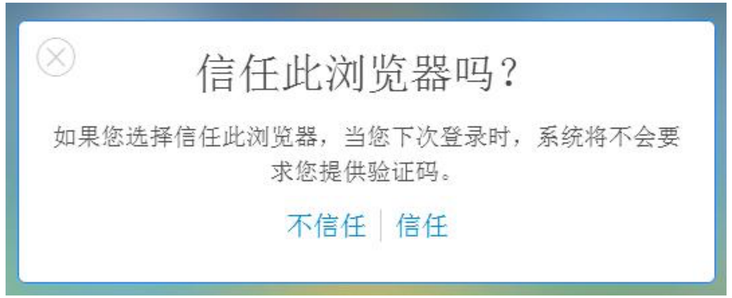
短信验证码存在重大缺陷

Google 二步认证方案将用手机提示取代短信验证码



Apple ID要开启两步验证

两步验证功能可以尽可能确保 Apple ID 和个人信息安全无虞



关注QCon微信公众号
获得更多干货!

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方：Geekbang. 极客邦科技 InfoQ