

# >> 解析P2P金融安全

# 关于我

乌云白帽子  
安全爱好者  
安全防御研究

2012-2015 当当网      网信金融

2015-今      万达电商

1

互联网金融及P2P简介

2

P2P日常安全解析

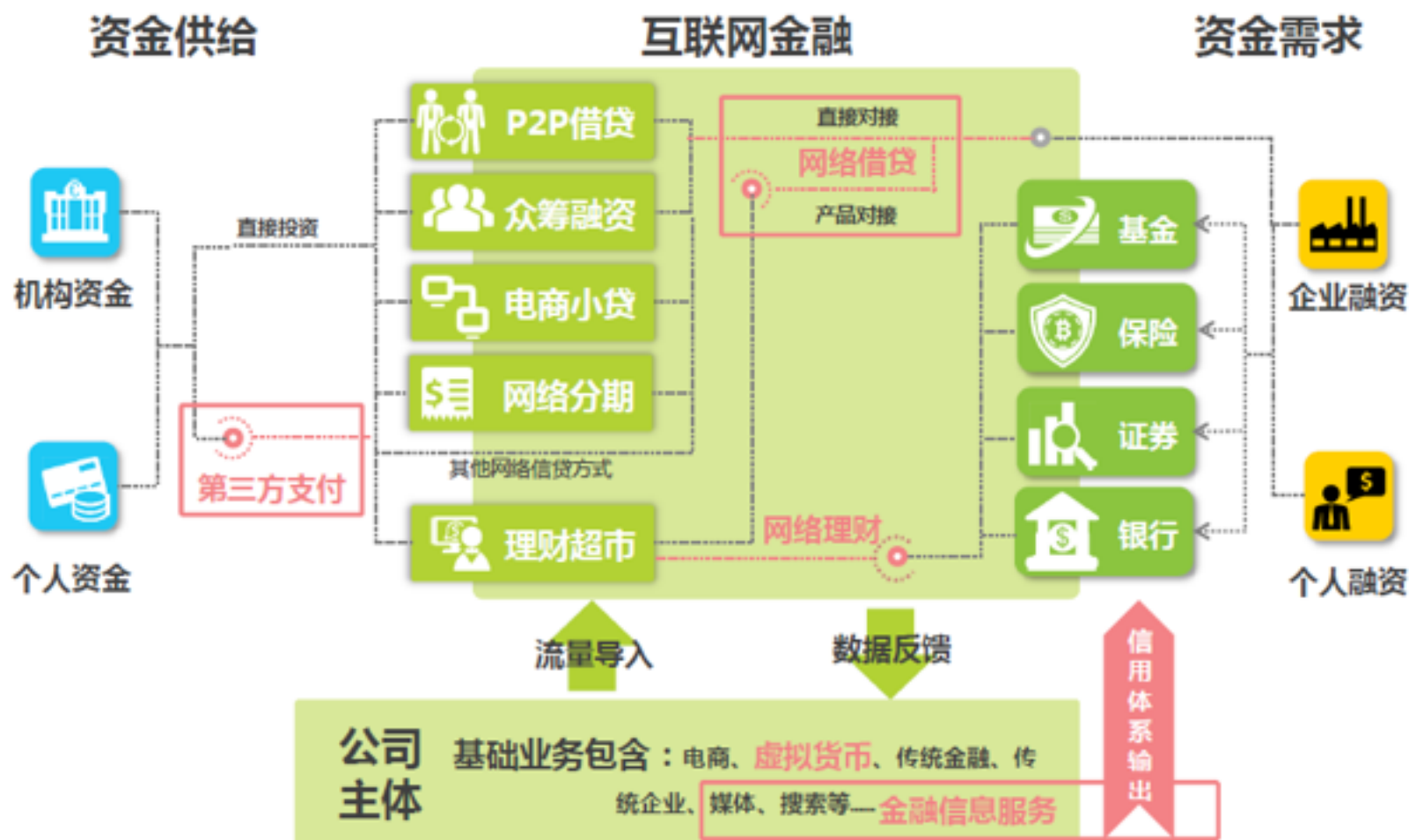
3

P2P业务安全解析

# 01

## 互联网金融及P2P简介

无论传统还是网络，金融的核心永远是资金融通



# 互联网金融三类玩家

## 互联网巨头

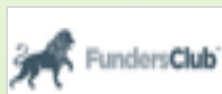
众安在线



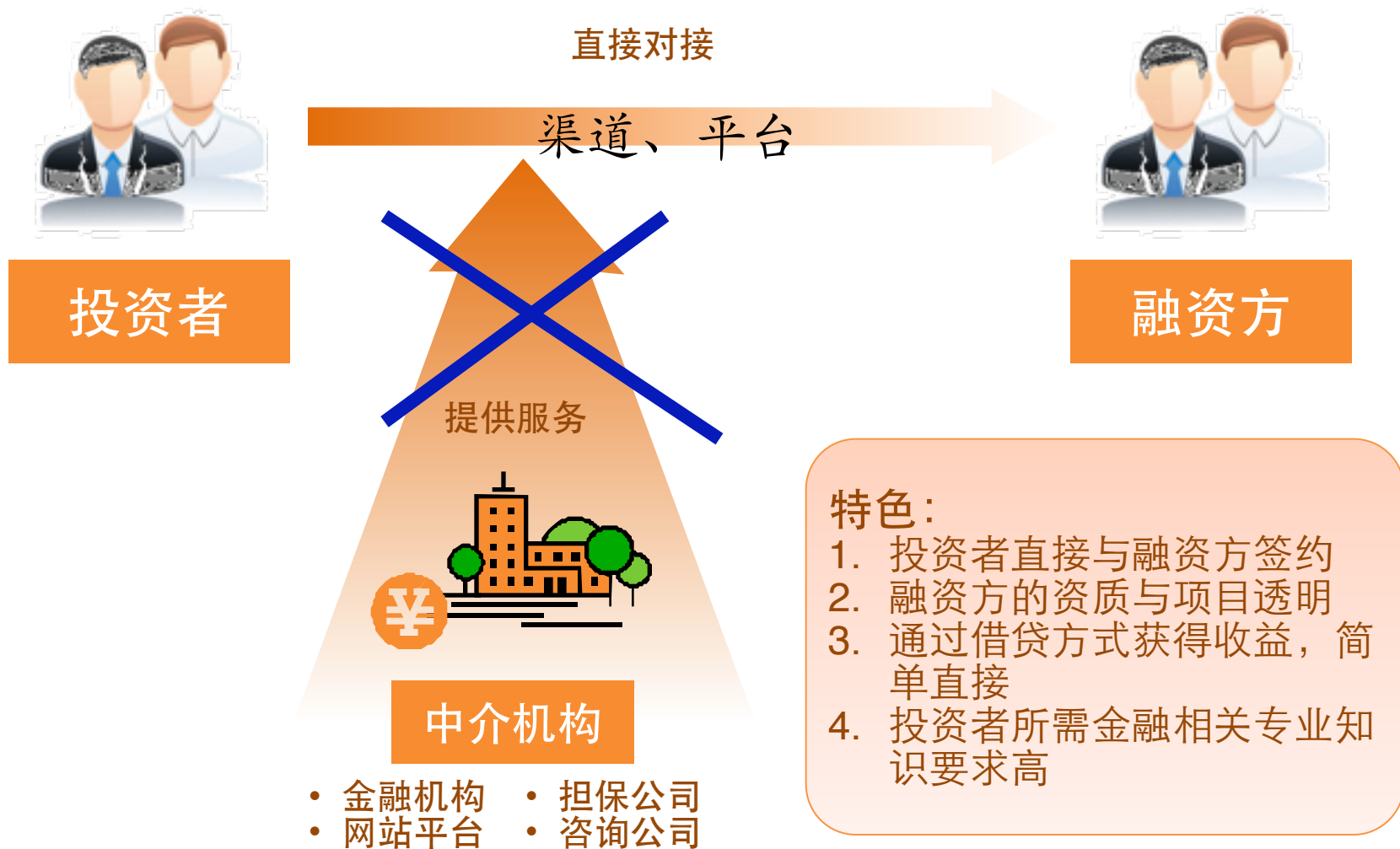
## 金融大佬



## 创新玩家



# P2P介绍



# P2P介绍



| 全部(2417)  |                      |      |          |                                       |     | 新手专享(468) | 产融贷(553) | 生财(216) | 房贷(553) | 应收贷(276) | 典当贷(46) | 租上租(66) | 医疗贷(14) | 其它(225) |
|---|----------------------|------|----------|---------------------------------------|-----|-----------|----------|---------|---------|----------|---------|---------|---------|---------|
| 投资项目  | 年化收益率                | 期限   | 还款方式     | 投资额度                                  | 状态  |           |          |         |         |          |         |         |         |         |
|  18万一口标, 乐融贷024<br>房贷 总额: 18.00万             | 9.5%                 | 6个月  | 按月付息到期还本 | 可投金额: 180,000.00元<br>借款预约中            | 预约中 |           |          |         |         |          |         |         |         |         |
|  100起投, 长兴2号001-17<br>企业贷 总额: 100.00万        | 8.00%+1.50%<br>APR专享 | 2个月  | 一次性还本付息  | 可投金额: 943,244.65元<br>剩余时间: 6天23时11分   | 投资  |           |          |         |         |          |         |         |         |         |
|  100起投, 长兴2号001-16<br>企业贷 总额: 100.00万        | 8.00%+1.00%<br>APR专享 | 2个月  | 一次性还本付息  | 可投金额: 986,657.18元<br>剩余时间: 6天23时50分   | 投资  |           |          |         |         |          |         |         |         |         |
|  定期20, 华夏1号008-28<br>租上租 总额: 0.80万           | 8.30%<br>APR专享+基础    | 177天 | 一次性还本付息  | 可投金额: 6,940.00元<br>剩余时间: 6天23时12分     | 投资  |           |          |         |         |          |         |         |         |         |
|  10万起投, 长兴2号001-14<br>企业贷 总额: 200.00万   | 8.00%+2.00%<br>APR专享 | 2个月  | 一次性还本付息  | 可投金额: 1,299,922.48元<br>剩余时间: 6天23时27分 | 投资  |           |          |         |         |          |         |         |         |         |
|  1万起投, 车易融162-4<br>车贷 总额: 100.00万      | 9.50%+0.40%<br>APR专享 | 6个月  | 按月付息到期还本 | 可投金额: 561,088.81元<br>剩余时间: 6天19时47分   | 投资  |           |          |         |         |          |         |         |         |         |

人人贷借款

信用等级 

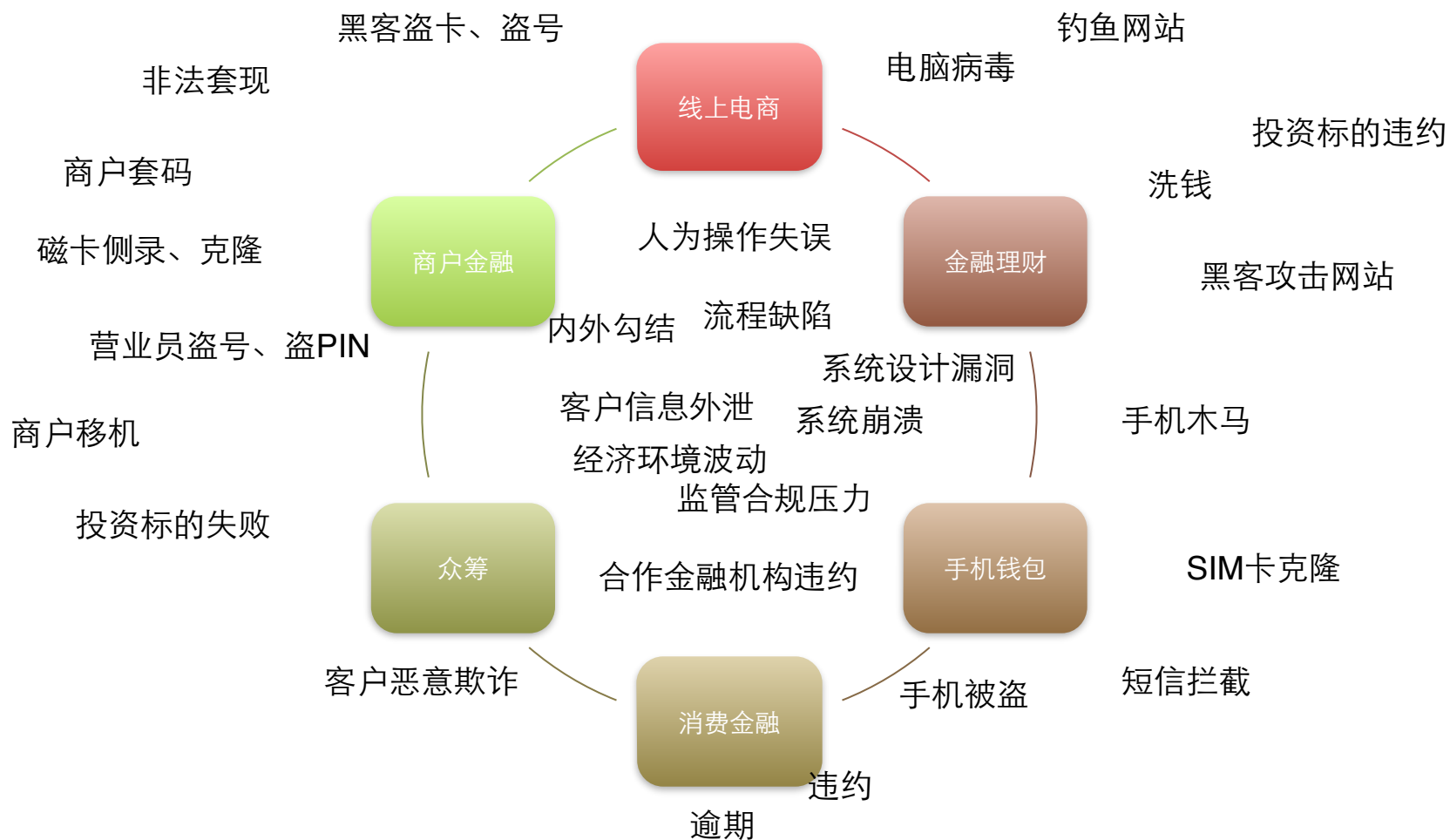
借款金额  元



| 借款期限   | 月综合费率 | 月还款额  | 总还款额      |
|--|-------|--|-----------|
|  3个月    | 0.88% | 17106.67元  | 51320.01元 |
|  6个月    | 0.88% | 8773.33元   | 52639.98元 |
|  12个月   | 0.88% | 4606.67元   | 55280.04元 |
|  24个月 | 0.88% | 2523.33元   | 60559.92元 |

申请借款





## 互联网安全风险

所有的互联网网站都面临的安全风险，如DDOS、web漏洞、密码破解、钓鱼等等；  
如何在快速迭代开发过程中保证web安全；  
接口风险，如支付、合作伙伴、认证接口等

## 金融安全风险

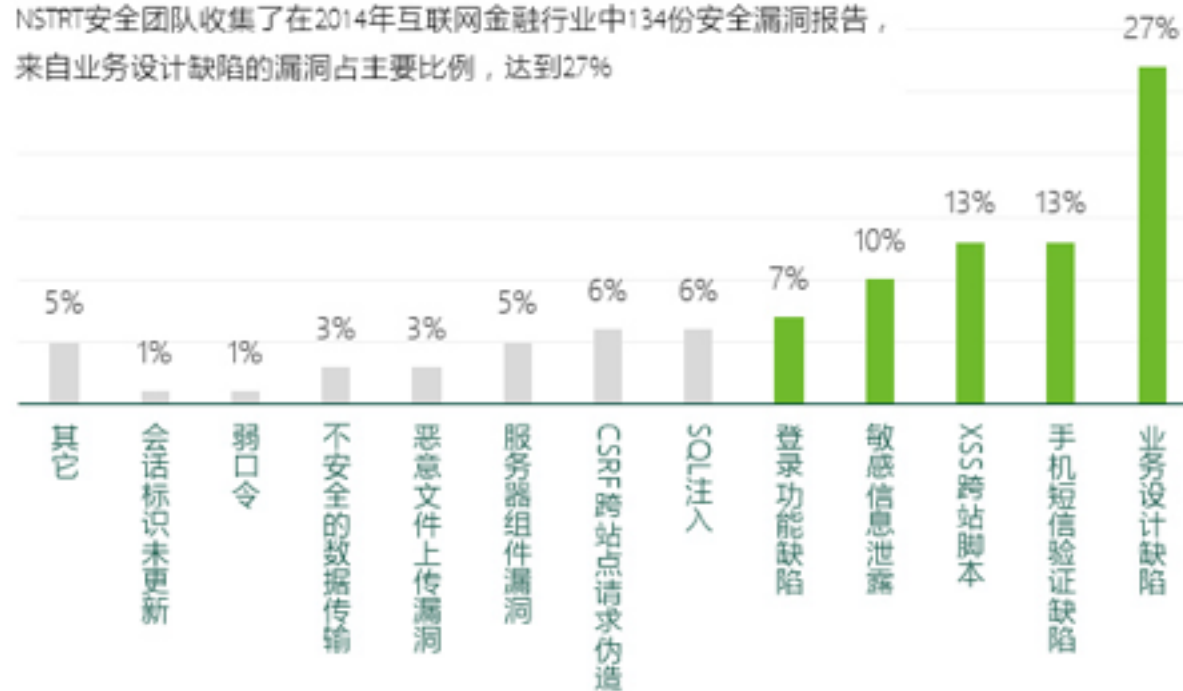
- 资金与支付风险；
- 用户身份仿冒、欺诈、套利、洗钱；
- 手机与APP风险；
- 内控与合规风险；
- 敏感信息泄露风险。

# 02

## P2P日常安全解析

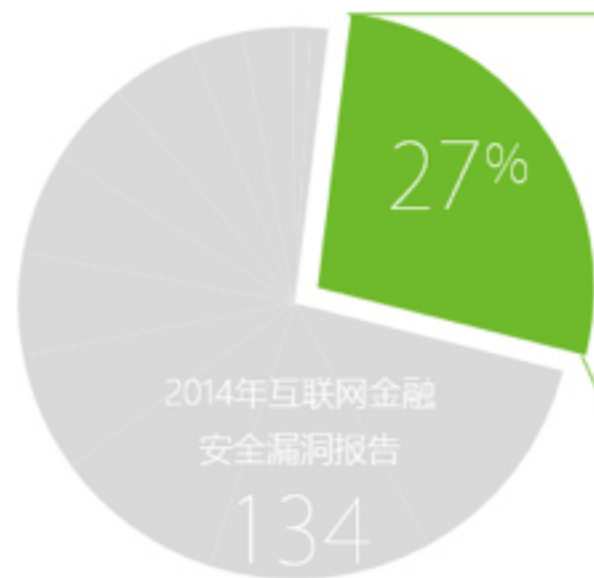
## 互联网金融安全漏洞统计

NSTRT安全团队收集了在2014年互联网金融行业中134份安全漏洞报告，来自业务设计缺陷的漏洞占主要比例，达到27%



Source : 2014 Internet FIN Security Report

[www.nsfocus.com](http://www.nsfocus.com)



互联网金融业务设计缺陷统计

|          |     |
|----------|-----|
| 平行越权查询   | 29% |
| 平行越权修改   | 20% |
| 垂直越权操作   | 7%  |
| 批量注册     | 7%  |
| 任意用户密码修改 | 7%  |
| 密码暴力破解   | 5%  |
| 平行越权下载   | 5%  |
| 身份伪造漏洞   | 2%  |
| 退出功能失效问题 | 2%  |
| 任意邮箱注册漏洞 | 2%  |
| 邮箱激活功能漏洞 | 2%  |
| 刷积分漏洞    | 2%  |
| 提现密码暴力破解 | 2%  |
| 邀请码暴力破解  | 2%  |
| 一号多户问题   | 2%  |
| 其它       | 4%  |

GITHUB

集团/边界

DDOS

# 03

## P2P业务安全解析

# P2P业务流程







# 分工明确

咱们这里分为 3 种会员 1 普通会员 99 元 2 高级会员 168 元 至尊会员 300 元 +  
普通会员保证金：99 元，拍满 400 单 平台返还 70 元 +  
高级会员保证金：168 元 拍满 300 单 平台返还 168 元（全额返还） +  
至尊会员保证金：300 元 拍满 300 单 平台返还 300 元（全额返还） +

【普通会员】普通会员 99： 只能拍单子 在做满 400 单后，平台会以奖励形式返还你 70 元。 +

（正常拍单所有单子都能做 不能做培训 客服 主持 接待）。 +

【联盟】 :52:50 +

【高级会员】正常拍单所有单子都能做（高级会员还有 4 大权限） +

1. 可以提升做红马管理，接待，培训，主持， +
  2. 优先做单权 特殊高佣金的单子一单可以赚到 15-20 +
  3. 就是优先推荐成为淘宝客服 +
  4. 高级会员专享淘宝专业导师开店指导免费公开课程（帮你实现开店创业梦想） +
- 咱们分销部 免费培训淘宝开店，从开店第一步，到店铺装修，到货源 发货 都是一键代发 +

【至尊会员】至尊会员在高级会员的基础上，享有更多尊贵特权。 +

1. 优先提拔为公会管理，享有底薪+提成的待遇 +  
在线时间达到 3 个小时，底薪 1500+提成 +  
在线时间达到 5 个小时，底薪 1800+提成 +  
在线时间达到 8 个小时，底薪 2500+提成 +
2. 至尊会员做满 300 单，享有拍单厅管理特权 +
4. 享有至尊优先培训服务，（由平台金牌培训导师为你指导） +

妇女，学生居多

# 自给自足

关键字: (姓名证件号)

张斌

点击查询

|            | 姓名 | 性别    | 年龄  | 生日 | 身份证号码 | 手机号码 | E-MAIL                    | 家庭地址                  | 入住登记时间       | 操作                 |
|------------|----|-------|-----|----|-------|------|---------------------------|-----------------------|--------------|--------------------|
| gsgf84     | 郭良 | 137   |     |    | FD 63 |      | year99@sh163.n            | -                     | 2012-16      | <a href="#">详情</a> |
| region5    | 郭良 | 15026 | 005 | FF | 35    |      |                           | 陕西                    | 2012-3:52:38 | <a href="#">详情</a> |
| dfgest3    | 郭良 | 13524 | 92  | FF | 35    |      |                           |                       | 2012-3:55:17 | <a href="#">详情</a> |
| feegt5     | 郭良 | 1376  | 047 | FF | 35    |      | zob163                    |                       | 3-11         | <a href="#">详情</a> |
| rrer455    | 郭良 | 1872  | 973 | FF | 35    |      | lanagatae...@yahoo.com.cn | -                     | 58           | <a href="#">详情</a> |
| eetetety6  | 郭良 | 1820  | 757 | FF | 35    |      | unce_zm@...com.cn         | -                     |              | <a href="#">详情</a> |
| dfhhfg6565 | 郭良 | 18201 | 367 | FF | 35    |      | zhangbinhui20...63.com    | 上海柳埠路135弄32号103       | 201-13       | <a href="#">详情</a> |
| ffdger78   | 郭良 | 13472 | 376 | FF | 35    |      | lina_pan@163              | -                     | 2012-9:39:18 | <a href="#">详情</a> |
| yrfhdf6    | 郭良 | 18217 | 024 | FF | 35    |      | army_707...com            | -                     | -12-14       | <a href="#">详情</a> |
| tgerh2015  | 郭良 | 18215 | 429 | FF | 35    |      | tianfan8...3.com          | -                     | 23:48        | <a href="#">详情</a> |
| drhrerh66  | 郭良 | 13116 | 480 | FF | 35    |      | ronzha...5@yahoo.com.cn   | 上海市普陀区贵门路460-23       | 11-15        | <a href="#">详情</a> |
| dfdf5554   | 郭良 | 18378 | 681 | FF | 35    |      |                           |                       | 1:05         | <a href="#">详情</a> |
| dfgghg899  | 郭良 | 18378 | 395 | FF | 35    |      | jimafanie...ina.com       | -                     | 2012-21      | <a href="#">详情</a> |
| fdffg54    | 郭良 | 18775 | 167 | FF | 35    |      | yudong...@126.com         | 浦东新区惠东镇新龙路489弄11号102室 |              | <a href="#">详情</a> |
| region5    | 郭良 | 15026 | 005 | FF | 35    |      | jumping...@163.com        | -                     | 2012-24      | <a href="#">详情</a> |

# 打码平台



我喜欢的卖家 钻石以上 | 我的消费主张 高品质



美团 苏宁 京东 陌陌 YY 微信 巨人 国美 小米  
验证码等 自动发码  
极速电信卡 给我留言

¥ 0.10

运费: 0.00

广东 汕头

43人付款 33人收货  
14条评论

账号 工具 设置 其它 ☐ 置顶

项目: 当当网手机注册

搜

获取数量: 2

获取号码

停止获取

收货

| 序号 | 手机号         | 验证码  | 状态          |
|----|-------------|--|-------------|
| 1  | 15976885014 |  | 第5次获取, 暂未收到 |
| 2  | 13418510182 | (...)尊敬的顾客, 欢迎注册当当网, 您申请的短信验证码为: a0731f, 请在页面填写。如非本人操... | 第1次获取, 获取成功 |

收货



验证码等 自动发码  
微笑ip鱼 给我留言

运费: 0.00

14条评论



美团 苏宁 京东 陌陌 YY 微信 巨人 国美 小米  
验证码等 自动发码  
雅友茶庄 和我联系

¥ 0.10

运费: 0.00

福建 厦门

36人付款 25人收货  
17条评论



注册验证码卡淘宝注册卡欠费卡短信卡联  
通卡手机上中信卡卡器设备

¥ 1.00

运费: 0.00

广东 潮州

2人付款 2人收货  
64条评论

# 内外勾结

银行-----羊毛党

羊毛党-----平台

# 对应办法

■最主要的是从业务角度防套利，不能让人“空手套白狼”；

■羊毛党心态：防止被平台反撸

■减少收益，提高收益门槛

■人工识别（客服挂电话）

■机器识别

■大数据应用

```
accuracy:0.96(260.000000/271.000000)
Suspicious User:
frhrr44
drgrr43
ljkhg6
dgdg343
uyedeg5
fgrt446
ffi878
fgsdhg235
dfgfhf66
dght577
dgdffhr4
dgdgeg54
heerrfg6
seet3445
```

```
and 1=1 union select 1,2,3 : malicious
select the best student union : legit
select * from admin : legit
'or 'x'='x' : malicious
```

## 2绑卡

■验证姓名与身份证号:利用公安部接口校验身份证信息

■绑卡阶段:银行预留姓名

|  |    |       |     |    |    |
|--|----|-------|-----|----|----|
| gsgf84   | 郭良 | 137   | FD  | 63 | 7  |
| region5  | 郭良 | 15026 | 005 | FF | 35 |
| dfgest3  | 郭良 | 13524 | 921 | FF | 35 |
| feegt5   | 郭良 | 1376  | 047 | FF | 35 |
| rrer455  | 郭良 | 1872  | 973 | FF | 35 |
| eetetety6  | 郭良 | 1820  | 757 | FF | 35 |
| dfhhfg6565   | 郭良 | 18201 | 367 | FF | 35 |
| ffdger78   | 郭良 | 13472 | 376 | FF | 35 |
|  | 郭良 | 18217 | 024 | FF | 35 |
|  | 郭良 | 18217 | 429 | FF | 35 |
|  | 郭良 | 13116 | 480 | FF | 35 |
| 网银U盾 银行卡 身份证 手机卡 开户单<br>工商700 建设500 农行700 广发 兴业 浦发 中信 交通等400-500 |    |       |     |    |    |
|  | 郭良 | 18775 | 167 | FF | 35 |
| region5  | 郭良 | 15026 | 005 | FF | 35 |



# 对应办法

■四要素验证：身份证，银行预留手机，姓名，银行卡号

■小额打款验证



3充值

5回收资金

■ 支付漏洞

■ 同卡进出

■ 资金闭环

■ 对账系统

## 4购买理财

geo集奥聚合

Copyright 2015 GEO SAS. All Rights Reserved. | www.geodata.com 99

P2P人群以男性为主

家庭稳定性

男女比例

在18点时上网活跃度达到峰值

- 对于P2P人群来说，在18点取到活跃度最高值；
- 除后斗

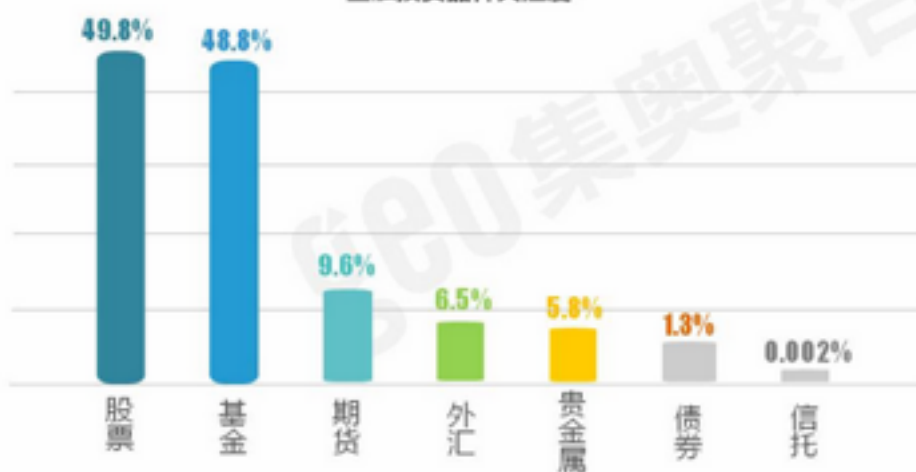
微信人群渗透率高于微博

- 在P2P人群中，使用微信的UV是微博UV的6.9倍。



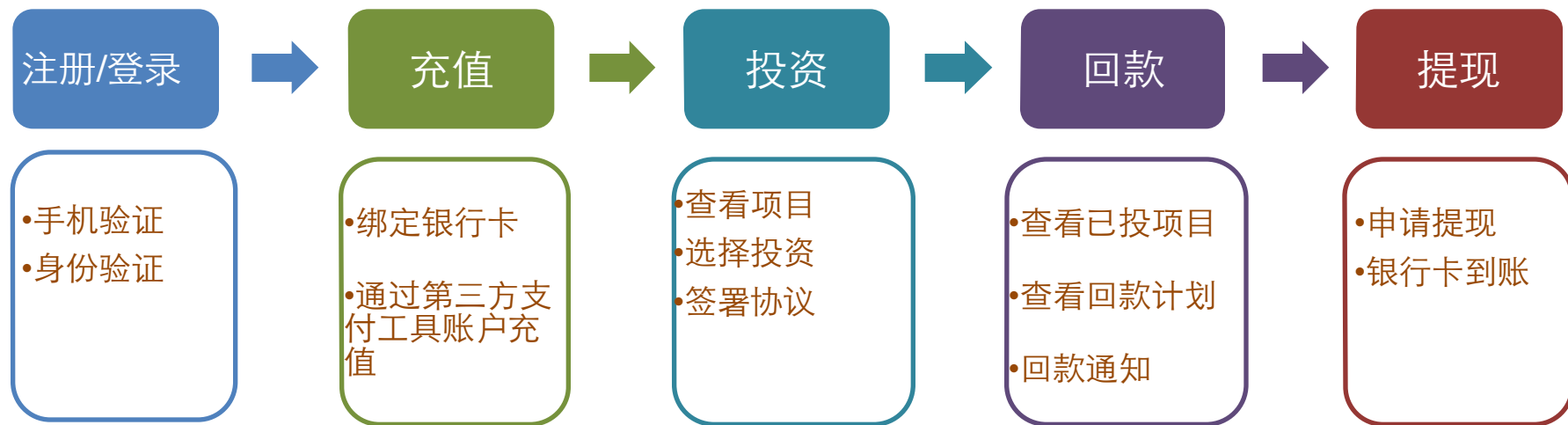
股票和基金是最受关注投资品种

金融投资品种关注度



## 4购买理财

### • 正常的用户行为：



## 4购买理财

- 异常的用户行为：



# 钓鱼

攻击成本分析：

构建网站成本+法律风险成本（？）

某银行网银用户总量 $m$ （几百万-3000万）

手机用户总量 $n$ （5亿个手机）

上当的概率 $p$ （万分之一）

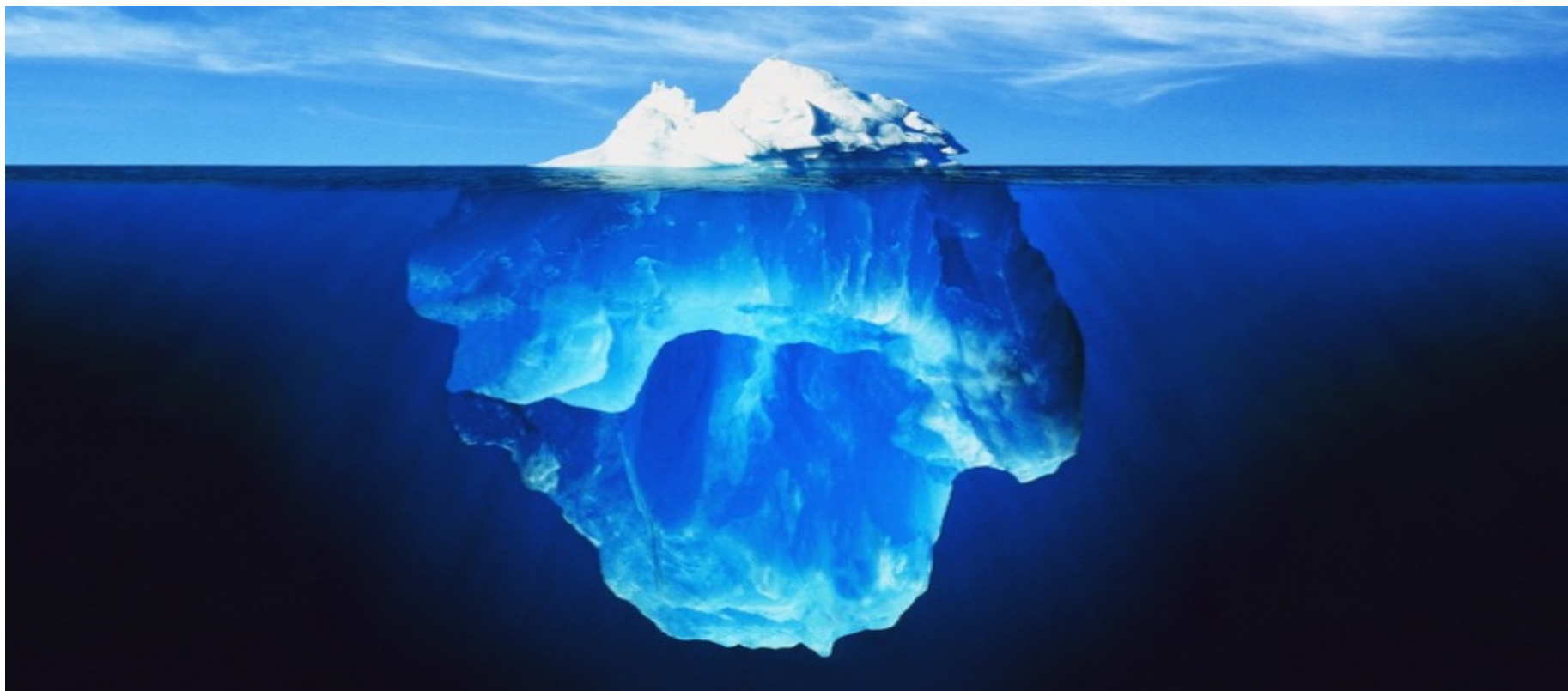
一条短信价格 $a$ （5分）

钓一条鱼成本

信息泄露---钓鱼



$$X = a / (p * m / n) + ?$$



Tank you ! >>

