>>)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 互联网金融及P2P简介

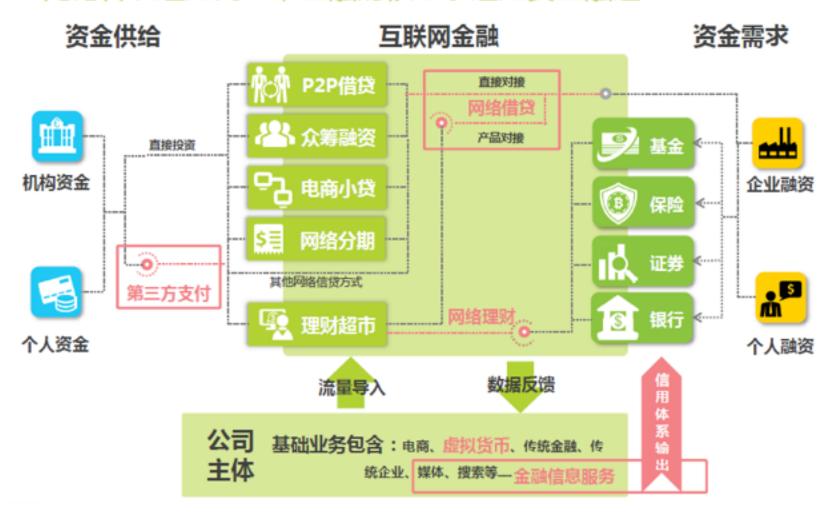
P2P日常安全解析

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















金融大佬







创新玩家















银联在摄























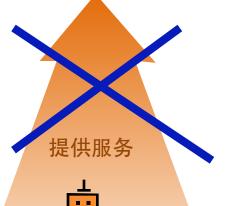
P2P介绍



投资者

直接对接

渠道、平台



中介机构

- 金融机构
 - 担保公司 网站平台 • 咨询公司



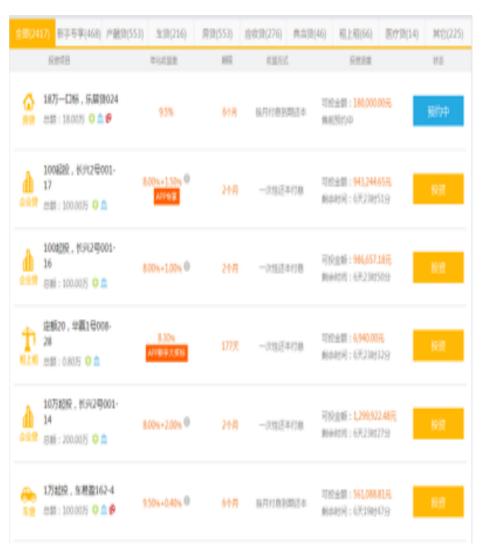
融资方

特色:

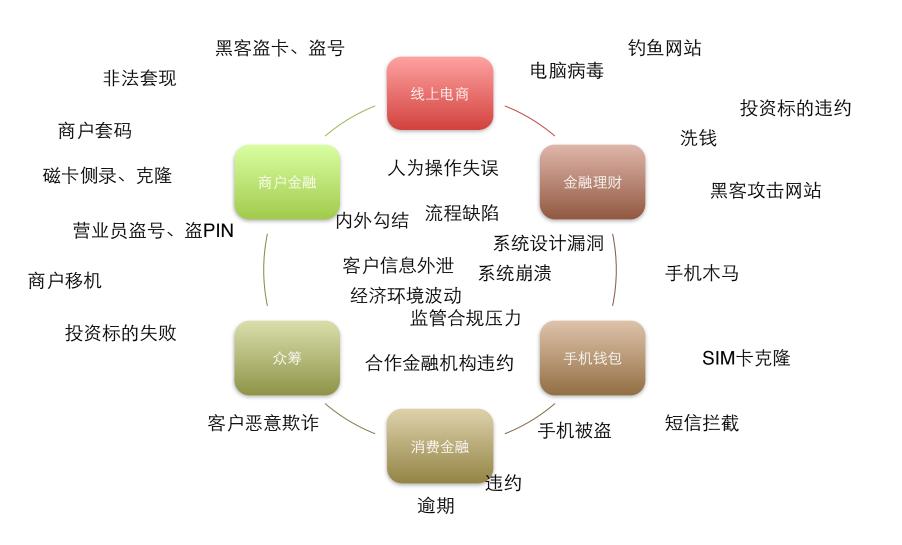
- 1. 投资者直接与融资方签约
- 融资方的资质与项目透明 2.
- 3. 通过借贷方式获得收益,简 单直接
- 投资者所需金融相关专业知 识要求高



P2P介绍







互联网安全风险

金融安全风险

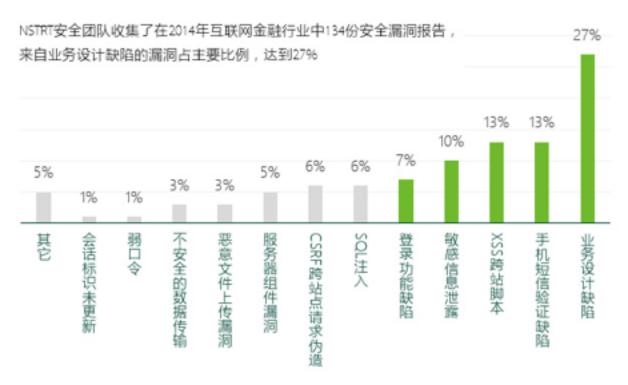
- 资金与支付风险;
- 用户身份仿冒、欺诈、套利、洗钱;
- 手机与APP风险;
- 内控与合规风险;
- 敏感信息泄露风险。



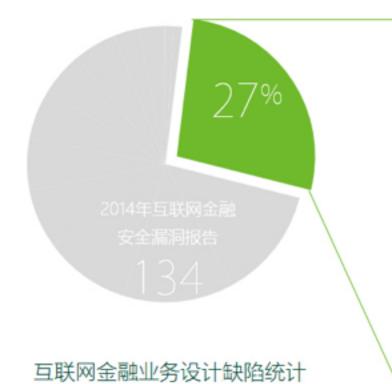
02

P2P日常安全解析

互联网金融安全漏洞统计



Source: 2014 Internet FIN Security Report www.nsfocus.com



平行越权查询	29%
平行越权修改	20%
垂直越权操作	796
批量注册	796
任意用户密码修改	796
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	296
任意邮箱注册漏洞	296
邮箱激活功能漏洞	296
刷积分漏洞	296
提现密码暴力破解	2%
邀请码暴力破解	296
一号多户问题	296
其它	496

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<u>单所有</u>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, 4
- 2. 优先做单权 特殊互相全面单本一单可以赚到
- 3. 就是优先推荐成为沙宾客服
- 4. 高级会员专享淘宝专业导师升店指导免费公开课程(帮你实现开店创业多想) 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↓
- 享有至尊优先培训服务,(由平台金牌培训导师为你指导)→

自给自足

良

良

18378

18378

18777

15020

dfdf5554

dfgghg899

fdffg54

region5

姓名 性别 生日 身份证号码 家庭地址 年龄 手机号码 E-MAIL 入住登记时间 良 137 63 gsgf84 FD 2012-1 year99@sh163.n 16 良 005 FF 35 region5 15026 2012 3:52:38 孠 PP 25 dfgest3 13524 2012 郭 良 ₹76¢ feegt5 3-11 n1 郭 良 rrer455 28 anagatae. Byahoo.com.cn 良 1820 757 eetetety6 FF E5 ince_zm@s 良 dfhhfg6565 18201 367 FF 35 201 13 _hangbinhui26 63.com 上海柳埠路135弄32号103 良 ffdger78 13472 376 FF 35 lina_pan@163 2012 9:39:18 良 vrfhdf6 18217 024FF. -12-14 army_707-23:48 良 18217429 FF tgerh2015 tianfan84 3.com all. 良 drhrerh66 13116 480 FF

11-15

1:05

20 21

13 1

20 7-24

1. 5

n1

5@yahoo.com.cn 上海市菩陀区费门路460-23

102室

浦东新区高东镇新龙路489弄11号

-27 µimafanle" ina.com

1@126.com

yudongy

关键字:(姓名/证件号)

FF

FF

FF

FF:

681

395

167

005

05

15

10070233 130002

张斌

打码平台

6

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

极速电信士 分给我留言

¥ 0.10 运费: 0.00 广东 汕头

43人付款 33人收货 14条评论

战 账号 工具 设置 其它 置頭 当当网手机注册 接 获取号码 停止获取 **获取数量:2** 状态 序号 手机号 验证码 第5次获取, 暂未收到 15976885014 木粒证码等 目切友码 运费: U.UU マツボドドビ 御笑ip曲 分给我留言 ¥ 0.10 福建 厦门 美团 苏宁 京东 陌陌 YY 徽信 巨人 国美 小 36人付款 25人收货 17条评论 运费: 0.00 米验证码等 自动发码 雅友茶庄 电和现联系 ¥ 1.00 广东 潮州 2人付款 2人收货 注册验证码卡淘宝注册卡欠费卡短信卡联 64条评论 运潮: 0.00 涌上较劲上由信上十分世代



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
fart446
ffi878
fgsdhg235
dfgfhf66
dght577
dgdfhr4
dgdgeg54
heerrfgf6
seet3445
```



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

gsgf84

region5

郭

■绑卡阶段:银行预留姓名

PSSS SPSP SPSP SPSP SPS

	0	10000	V ~	25000		10000		
	dfgest3	郭	良	13524	921	FF	35	7
	feegt5	郭	良	1376)47	FF	35	5
	rrer455	郭	良	1872	373	FF	£5	5
	eetetety6	郭	良	1820	757	FF	£5	J
	dfhhfg6565	享	良	18201	367	FF	35	5
	ffdger78	享	良	13472	376	FF	35	5
	211111	享	良	18217)24	FF.	15	5
	NAME OF TAXABLE	享	良	18217	429	FF	5	5
::::::		享	良	13116	480	FF	.5	5
F#1 F1	E to Traverse	100	银U盾(限行卡 身	份证书	F机卡	开户单	5
2 (注	99字、开广员料率、 9宝交易,代收货款。	工发	.商700 弘 : 中信 3	建设500 才 运通等400	マ行700 -500	广发	き 兴业 浦	5
533	3	郭	₹	18777	167	FF	ō	5
3-	-6563 region5	亨	Ą	1502€	005	FF:	.5	5

137

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

■支付漏洞

■同卡进出

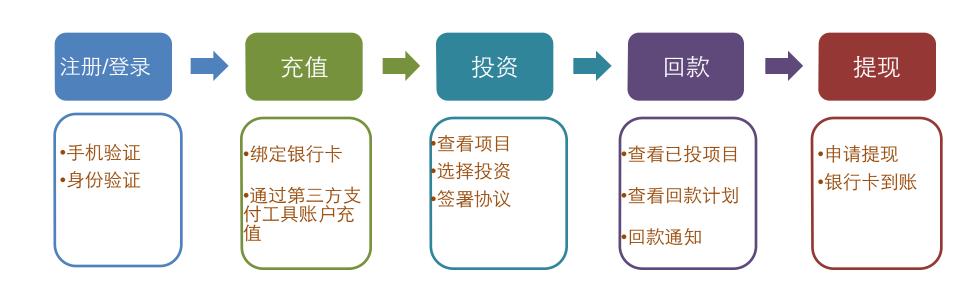
■资金闭环

■对账系统

购买理 财



• 正常的用户行为:



• 异常的用户行为:

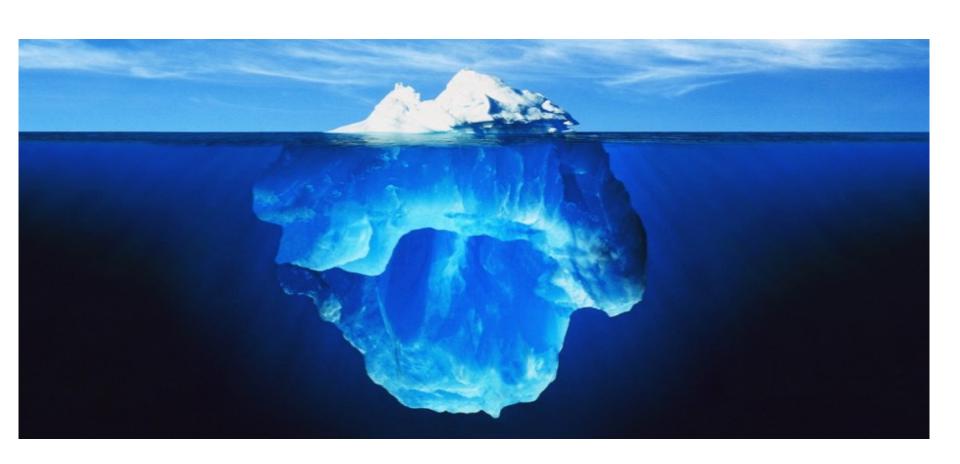


钓鱼



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





Tank you! >>>



