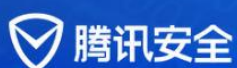


腾讯安全2018上半年 互联网金融安全报告



目录

引言

一、互联网金融风险态势分析

1. 市场监管“严上加严”，加速创建“无传销网络平台”
2. 严厉打击外汇违法违规行为，维护市场良性秩序
3. P2P 行业面临洗牌，或迎来发展分水岭

二、互联网金融安全风险的主要类型

1. 非法集资涉案金额超千亿，隐蔽和欺骗性增强
2. 网络传销活跃参与人数超千万，金融理财类传销成主流模式
3. P2P 网贷整顿力度加大，行业监管日趋严格
4. 互联网外汇交易违法嫌疑大，基金与贵金属交易深受影响
5. 非法金融平台投资骗局多，为招揽投资者虚假宣传

三、安全行业防范互联网金融风险的技术手段与典型应用

1. 钓鱼网站检测方法
2. 打击通讯信息诈骗
3. 伪基站识别技术
4. 服务端预警系统

四、防范互联网金融风险安全建议

1. 提升金融安全防范意识
2. 安装安全软件实时开启防护

引言

金融是现代经济的命脉，直接关系到国家经济的繁荣、稳定和发展。近年来，大数据、云计算、人工智能和区块链等创新技术通过优化金融业务流程、降低交易成本、减少信息不对称、拓展交易可能性集合、升级金融基础设施，进一步推动金融业朝精细化方向发展，并一定程度上缓解了中小企业融资难、融资贵问题，助力普惠金融提质增效。

然而，在互联网金融快速发展的同时，各种金融领域的诈骗手法、擦边球模式也逐渐进入公众视野，从传统的以信用卡代办、小额贷款办理为由骗取小额手续费，到各种如非法集资、非法外汇交易、非法贵金属等期货交易、荐股类诈骗等。

特别是金融诈骗引入传销手法，更是危害严重，比如虚拟币传销、非法集资传销、商城返利传销等。据腾讯安全反诈骗实验室监测数据显示，2018 年上半年发现涉嫌传销平台 3000 多家，高风险金融平台 1 万多家，针对监管部门已经定性的传销、金融诈骗类网站，腾讯安全在所有覆盖渠道拦截，日均拦截访问达千万次。

传统的金融监管手段正遭遇前所未有的挑战：通过网络实现的新型传销和非法集资案件频发，几乎每一个传销盘和集资盘都有看似高大上的网站和 APP，具备很强的迷惑性。老百姓在缺少基本的金融背景知识的情况下，很难辨别其中的陷阱。同时，在监管整治与宏观经济去杠杆的双层作用下，P2P 行业进入洗牌阶段，公安部针对金融诈骗、非法集资与传销等金融犯罪也保持一以贯之的严打高压态势。

基于互联网金融行业安全态势以及监管现状，腾讯安全《2018 上半年互联网金融安全报告》就如何认识互联网金融新型风险、寻求互联网金融风险防控技术与实务结合、更好地保护网民权益进行了梳理，以期达成行业共识，有效防范风险、维护互联网金融安全稳定，促进普惠金融落到实处。

一、互联网金融风险态势分析

1. 市场监管“严上加严”，加速创建“无传销网络平台”

针对网络传销日趋蔓延的严峻形势，新组建的国家市场监督管理总局于 2018 年 4 月 3 日发布《关于进一步加强打击传销工作的意见》（http://samr.saic.gov.cn/xw/yw/wjfb/201804/t20180409_273591.html）。《意见》指出，今年各级工商和市场监管部门要大张旗鼓开展“无传销网络平台”创建工作，作为探索应对网络传销泛滥蔓延的一项重要举措。通过对网络传销传播的重要载体——互联网平台实施积极引导和监管，压实互联网平台企业责任，减少网络传销信息源，切断网络传销传播扩散渠道，深度净化网络空间，营造风清气正的网络环境。

“无传销网络平台”创建工作以深圳网络传销监测治理基地与腾讯微信平台监测合作为起点。同时，根据 2017 年传销举报投诉情况，将廊坊、北海、南宁、南京、武汉、长沙、南昌、贵阳、合肥、西安、桂林市列为 2018 年传销重点整治城市。重点城市名单每年更新一次，国家市场监督管理总局竞争执法局适时对重点城市开展督导检查 and 验收，并根据情况对名单进行调整。对整治工作长期不见起效的城市可直接约谈党政主要领导，责令限期整改，并在一定范围内予以严肃通报批评。4 月 8 日又发布《国家市场监督管理总局关于进一步加强直销监督管理工作的意见》，加强直销监管，依法查处与直销相关的各类违法行为；4 月 24 日，再发《市场监管总局办公厅关于开展查处以直销名义和股权激励、资金盘、投资分红等形式实施传销违法行为专项行动的通知》，提出从 5 月开始，组织全国工商和市场监管部门开展查处以直销名义和股权激励、资金盘、投资分红等形式实施传销违法行为专项执法行动。打击传销作为 2018 年各监管部门的一项重点工作，政企合作将为监管部门提供强有力的数据与技术支持，助力对于金融传销犯罪的“打早打小”，降低群体性金融风险，遏制网络传销蔓延。

2. 严厉打击外汇违法违规行为，维护市场良性秩序

针对名目众多的网络投资项目如外汇、贵金属、期货、指数等产品在线交易，中国互联网金融协会于 2017 年 11 月 10 日发布《关于防范通过网络平台从事非法金融交易活动的风险提示》，明确指出了境内机构未经我国金融监管部门批准通过互联网站、移动通讯终端、应用软件等各类网络平台从事外汇、贵金属、期货、指数等产品交易（含跨境），以及境外机构未经我国金融监管部门批准通过互联网站、移动通讯终端、应用软件等各类网络平台为境内客户提供外汇、贵金属、期货、指数等产品交易，均属于违法行为。以此为依据，腾讯灵鲲大数据金融安全平台对监测到的数千家平台实行全网拦截，有效降低了用户访问此类网站的风险。

3. P2P 行业面临洗牌，或迎来发展分水岭

针对 P2P 行业的监管日趋严格。2017 年 12 月 13 日，银监会 P2P 网络借贷风险专项整治工作领导小组办公室下发《关于做好 P2P 网络借贷风险专项整治整改验收工作的通知》，通知要求，各地应在 2018 年 4 月底前完成辖内主要 P2P 机构的备案登记工作，6 月底之前全部完成；并对债权转让、风险备付金、资金存管等关键性问题作出进一步的解释说明。

2018 年的备案对 P2P 网贷意味着大洗牌，也是行业从野蛮发展走向合规理性的分水岭。北京、上海、南京、深圳、浙江、重庆等地纷纷出台针对互联网金融以及非法集资的整治措施。在一轮又一轮的全面摸底调查之后，各地方细则渐趋完善。互联网金融行业的洗牌将会随着监管的趋紧而加速，P2P 行业整体风险也会趋于稳定、更为可控。

二、互联网金融安全风险的主要类型

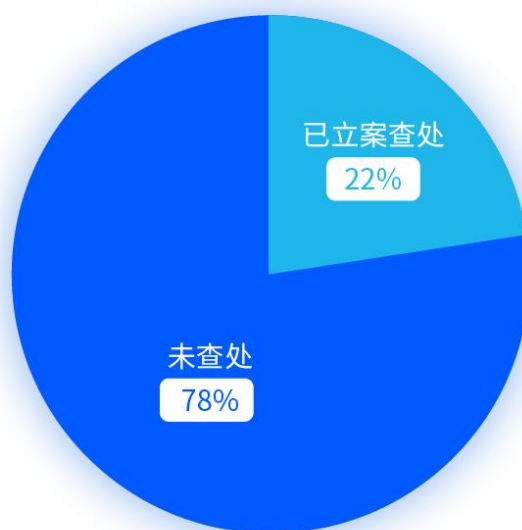
1. 非法集资涉案金额超千亿，隐蔽和欺骗性增强

非法集资是指未经有关部门依法批准，承诺在一定期限内给出资人还本付息，向社会不特定对象即社会公众筹集资金，同时，以合法形式掩盖其非法集资的性质。非法集资活动具有很大的社会危害性，使参与者遭受经济损失，严重干扰正常的经济、金融秩序，极易引发社会风险等。近年来，非法集资案件发案数量增多，形式越发多样，隐蔽性和欺骗性也越来越强，非法集资涉案金额超千亿，给国家的金融、社会秩序造成极大的破坏。

上海检察院发布金融检察白皮书显示，2017 年，检察机关受理的非法集资案件数量继续高位攀升，涉众型犯罪风险突出。一方面是受理案件数量高位运行，另一方面大案、要案频发，涉及金额巨大，仅“e 租宝”、“申彤大大”、“中晋系”、“快鹿系”、“善林系”五大系列案件，涉案金额就将近 2000 亿元人民币。其中，“善林金融”实际控制人周伯云以允诺年化收益 5.4%至 15%不等的高额利息为饵，向社会不特定公众吸收资金，涉案金额近人民币 600 亿元，于 2018 年 4 月 24 日被批捕。

截至 2018 年 6 月，腾讯灵鲲大数据金融安全平台累计发现网络非法集资平台一千余家，目前已立案查处 200 余家。

非法集资平台



腾讯安全2018上半年互联网金融安全报告

数据来源: 腾讯灵鲲大数据金融安全平台



从注册公司所在地来看，主要集中在沿海发达地区如广东、北京、上海、江苏、浙江等。

非法集资公司注册地分布



广东	35%	浙江	4%	四川	3%	贵州	2%
北京	15%	湖南	4%	湖北	2%	河南	2%
上海	7%	山东	4%	辽宁	2%	重庆	2%
江苏	5%	福建	3%	陕西	2%	其他	8%

腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯灵鲲大数据金融安全平台



2. 网络传销活跃参与人数超千万，金融理财类传销成主流模式

近年来，以无接触、网络化、地域分散化为特征的新型传销开始频繁出现，监测到的传销平台三千多家，活跃参与人数达数千万。越来越多的金融平台通过传销的手法，借助互联网和社交网络快速发展壮大，风险等级呈指数级增长。

新型网络传销的主要模式包括：

1) 以高收益为诱饵的金融投资理财项目进行诈骗，涉案金额巨大，扰乱了社会经济秩序，危害国家经济安全以及公民个人经济利益，极易引发群体性事件等违法犯罪案件，已成为影响社会稳定的隐患之一。已经崩盘的钱宝网，项目年化收益率高达50%以上，其收益组成=任务收益+签到收益+推广收益+体验任务收益。其中，拉人头推广收益占了很大比例，从而吸引大量投资者蜂拥而至，涉案金额高达300亿，影响极为恶劣。

2) 各类境外资金盘、虚拟币、ICO项目层出不穷，很多都是打着创新的幌子，许以高额回报。其中蕴含非法发行、项目不实、跨境洗钱、诈骗、传销等诸多风险，造成大量资金流向境外，严重危害国家金融安全。由于不受国内机构监管，一旦崩盘、跑路或者失联，投资者往往投诉无门，损失难以追回。比如百川币、SMI、MBI、马克币、贝塔币、暗黑币、美国富达复利理财等等。

3) 打着“消费返利”、“消费多少返多少”、“消费增值”、“消费就是存钱”等口号的各类网上商城及线下商城，开始成为传销的新变种。已被查处的浙江万家购物网，打着“满500返500”等幌子诱使他人消费和入会，按照资格和条件，分为普通会员、VIP会员、金牌代理、金牌代理商、区域代理商等等级，实行层级计酬，涉案人员190万，金额高达240.45亿，遍及全国31个省（市、区）的2300多个县（市）。

4) 打着“精准扶贫”、“慈善互助”、“国家工程”、“民族大业”、“资本运作”等旗号，收取加盟费后承诺获取高额回报的（如年收益率高于20%），基本可以认定为传销。MMM金融互助平台宣称月收益率可以达到30%，此外，参与者发展他人加入可获得推荐奖（下线投资额的10%）、管理奖以及发展“下线”的管理奖：第一代5%、第二代3%、第三代1%、第四代0.25%，以此激励模式鼓励会员不断发展更多的下线。善心汇以“扶贫济困、均富共生”的名目，以高收益为诱惑，发展“会员”500多万名，涉案金额数百亿。

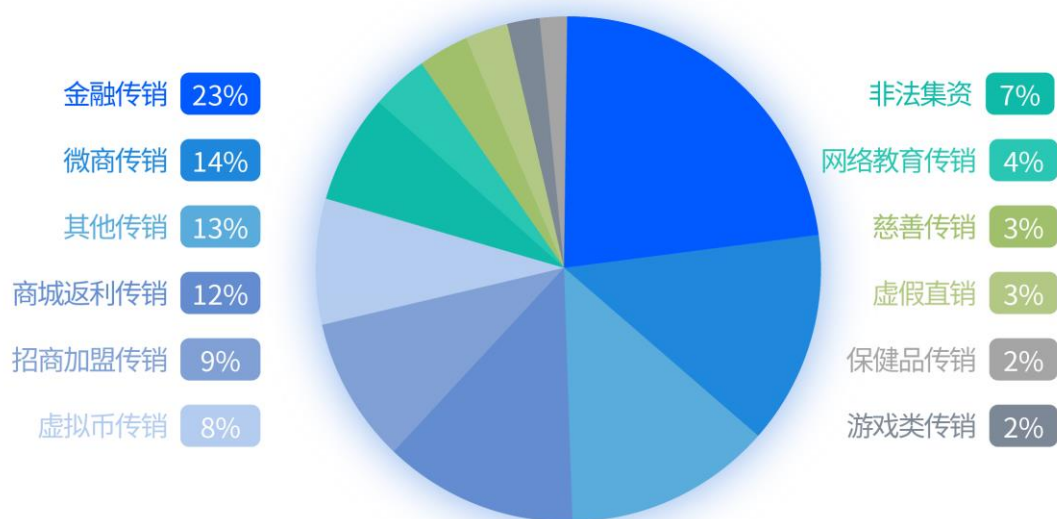
5) 以保健品、收藏品、投资等为载体的骗老陷阱：先以免费体检、产品体验、健康讲座等形式吸引老人参与，通过套近乎、亲情牌与老人拉近关系后，进行“洗脑”式推销。不仅给老人造成经济损失，还会影响其身心健康，进而破坏家庭和谐与社会稳定。

6) 打着“微营销”、“微商”等旗号，销售低质量、低成本商品甚至三无产品，通过发展社交平台好友成为下级，进行层级计酬。比如全国首例社交平台传销案——陈志华传销案，所谓的“亚洲催眠大师”陈志华，宣传交59800元代理费，每天只要转发营销课程，拉更多人来听课，就能“月入百万，108天买奔驰，6个月买房，一年开上劳斯莱斯”，该案涉案人员达329人，涉案金额达461万元。

7) 理财游戏类传销：以高额收益为诱饵，通过在游戏中充值获得固定奖励，推荐更多人参与，则可以获得更多的动态收益。已破获的“魔幻农庄”游戏传销，在短短5个月时间里，先后发展涉及重庆、四川、广东等28个省市的12万余名玩家，交易金额达4600余万元，最终全面崩盘。

从传销类型分布来看，金融投资类传销占比最多，紧接着是商城返利、招商加盟、微商旗号类、山寨虚拟币传销，金融投资类传销已发展成为新型网络传销的主流模式。

传销类型分布



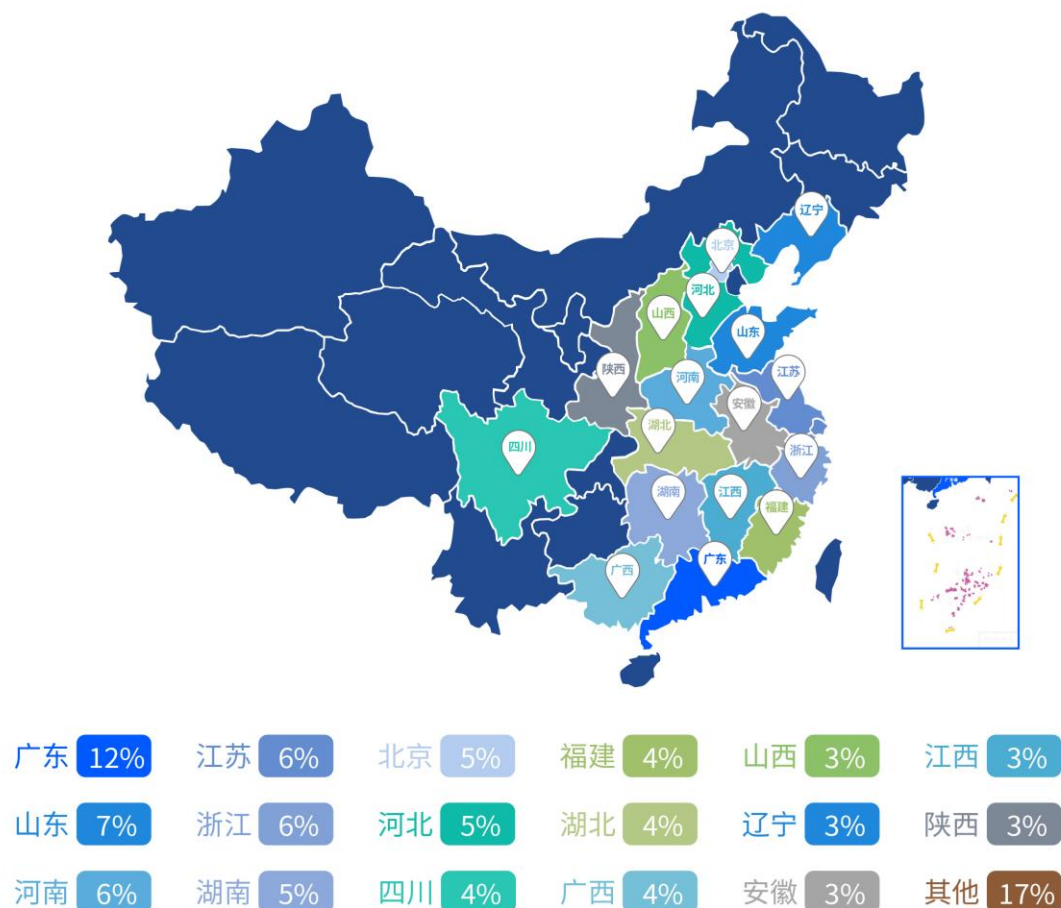
腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯灵鲲大数据金融安全平台



地域分布上看，传销参与者主要集中在广东、山东、河南、江苏、湖南、浙江等省。

传销参与者地域分布



腾讯安全2018上半年互联网金融安全报告

数据来源:腾讯灵鲲大数据金融安全平台

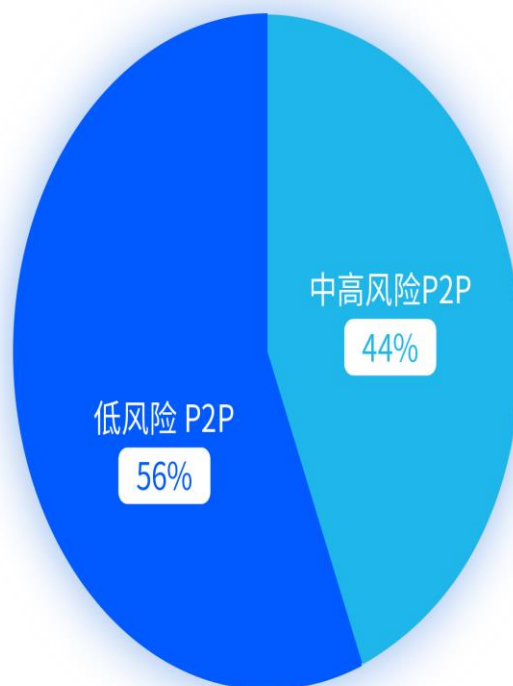


3. P2P 网贷整顿力度加大，行业监管日趋严格

2018 上半年，一批未经批准的 P2P 网贷机构从出现到跑路的消息不断传出，投资生态环境亟待整顿。许多地区 P2P 网贷机构的业务规模扩张受限，加上整体金融环境收紧、去杠杆力度加大，P2P 网贷逐渐进入行业洗牌阶段。

基于网贷平台的行业现状，政府有关部门加大了整治力度，协同安全企业，共同规范 P2P 行业规则。同时，安全行业也积极推动科技创新，尝试运用技术手段识别预警金融风险。腾讯灵鲲大数据金融安全平台累计发现 P2P 网贷机构 1 万余家，其中存在中高风险的占比约为 44%。

P2P平台风险情况



腾讯安全2018上半年互联网金融安全报告

数据来源:腾讯灵鲲大数据金融安全平台



从地域分布上看，P2P 网贷机构主要集中在广东、上海、北京、浙江、山东、江苏等省市。

P2P平台公司地域分布



广东 17%	山东 7%	安徽 2%	辽宁 2%	陕西 1%
上海 14%	江苏 5%	河北 2%	湖南 2%	江西 1%
北京 13%	福建 3%	河南 2%	广西 1%	山西 1%
浙江 10%	湖北 3%	四川 2%	重庆 1%	其他 11%

腾讯安全2018上半年互联网金融安全报告

数据来源:腾讯灵鲲大数据金融安全平台



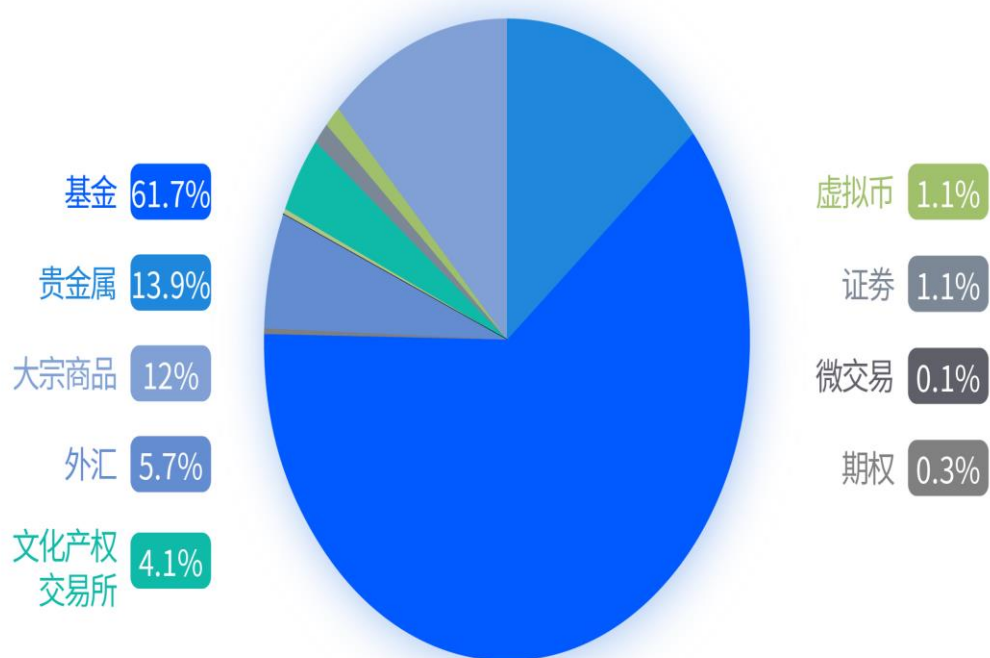
4. 互联网外汇交易违法嫌疑大，基金与贵金属交易 深受影响

互联网外汇、期权、期货、贵金属、大宗商品、文化产权、基金、证券、虚拟币等交易平台种类多样、名目繁多、隐患巨大。根据2017年11月中国互联网金融协会发布的《关于防范通过网络平台从事非法金融交易活动的风险提示》，境内机构未经我国金融监管部门批准通过的互联网站、移动通讯终端、应用软件等各类网络平台为境内客户提供外汇、贵金属、期货、指数等产品交易（含跨境），以及境外机构未经我国金融监

管部门批准通过互联网站、移动通讯终端、应用软件等各类网络平台为境内客户提供外汇、贵金属、期货、指数等产品交易，均属于违法行为。部分非法交易平台藏匿其中，真假难辨，严重危害了投资者的资金安全。

从已收录平台的数量情况占比来看，数量最多的是基金、贵金属、大宗商品、文化产权交易所等平台。

金融交易平台数量



腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯灵鲲大数据金融安全平台



从地域分布上来看，广东、上海、北京、浙江、江苏、山东等省市的金融交易平台数量较多。

金融交易平台公司分布



腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯灵鲲大数据金融安全平台



5. 非法金融平台投资骗局多，为招揽投资者虚假宣传

非法金融平台为了提高自身可信度，通过正规公司注册、网站注册、网站备案展开互联网业务，带来荐股诈骗、网络赌博、微盘二元期权、“虚假国家项目”等金融风险。这些非法金融活动平台有自己独特的推广方式和骗钱套路，以荐股为例，荐股机构通过

拉涨小盘低价股票骗取用户信任，再向用户推荐所谓的“必涨股”收取以收取会员费用，骗取用户资金。

从鉴股平台地域分布情况看，主要集中在广东、北京、上海等经济较为发达的地区，紧随其后的是湖北、江苏、福建、四川等省份。

荐股平台地域分布



腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯灵鲲大数据金融安全平台



三、安全行业防范互联网金融风险的技术手段与典型应用

在防范和监管金融黑产，助力政府打击、防范以金融创新之名行诈骗之实的普“恶”金融，以及非法集资、金融传销等涉众型金融犯罪等方面，安全行业提供了重要的技术支持。腾讯安全将业内常用的防范互联网金融安全风险技术手段梳理如下：

安全行业防范互联网金融风险 技术手段与典型应用

序号	类型	说明	典型应用
1	钓鱼网站检测	技术鉴定钓鱼网站及与其关系密切的站群，将网站域名加入钓鱼网站列表，当用户访问时通过杀毒软件或者浏览器进行直接拦截。	腾讯神荼反欺诈盒子
2	打击通讯信息诈骗	鉴定诈骗短信和诈骗电话，不断丰富诈骗来电号码库，实现快速鉴定和拦截，避免用户受到诈骗信息的骚扰。	腾讯鹰眼智能反电话诈骗系统、腾讯电脑管家
3	伪基站识别	伪基站被广泛应用于冒用公众服务号码或权威部门名义编造发送虚假信息，通过技术识别拦截伪基站短信，判断伪基站位置并协助警方打击犯罪。	腾讯麒麟伪基站实时定位系统
4	服务端预警系统	金融、传销风险态势感知和预警的解决方案，帮助用户、监管部门实现对金融风险平台的迅速反应。	腾讯灵鲲大数据金融安全平台、腾讯神侦资金流查控系统

1. 钓鱼网站检测方法

对付互联网金融欺诈网站最常用的方法，就是技术鉴定钓鱼网站，并将风险网站域名加入钓鱼网站列表，当用户访问时，实现让杀毒软件或浏览器直接拦截。

钓鱼网站往往具有家族特性，域名更换很快，钓鱼网站经营者会一次性注册很多个域名，还会将多个网站部署在同一个 IP 的服务器上，根据这些特性（注册者 ID、服务器 IP、域名等）可一次将一批钓鱼网站鉴别出来拉黑。

腾讯神茶反欺诈盒子通过大数据分析和机器学习，识别并拦截欺诈钓鱼网址，对典型的网址诈骗进行线索挖掘、团伙聚集分析，提供给有关部门做线下打击和抓捕。并形成活跃恶意网址库，借助腾讯产品客户端、运营商渠道及公安部门合作，从云、管、端实现对钓鱼诈骗网址的精准识别、提示与拦截。腾讯神茶系统目前已与多地警方、食药等执法部门合作，有效降低互联网案发率：南京无锡等部署地涉案数下降超过 60%；食药总局合作中，每天发现违法销售网站 3000 多个，阻断互联网虚假食药销售 100 多万次。腾讯神茶系统在南京公安落地的“金陵网盾”产品上线后，网络诈骗案件日平均发案同比下降 48%，拦截成功率达 98%，准确率达 99%以上。

2. 打击通讯信息诈骗

对于诈骗电话和诈骗短信，已经有非常成熟的鉴定方法。安全大数据会收集分析所有诈骗电话和短信，通过模糊特征匹配，实现快速鉴定和拦截。再配合用户主动举报、标记诈骗电话或短信，来不断丰富充实来电号码库。

腾讯鹰眼智能反电话诈骗系统解决日益猖獗的电话诈骗问题，其基于大数据分析，利用智能反诈骗引擎模型可实时测出正在受骗的用户，并通过警方或运营商对受骗用户进行劝阻，保障民众通讯安全。目前鹰眼系统已经通过与 6 省市公安部门、两大运营商、和 3 省市通管局合作，落地全国 20 多座城市，为人民通讯安全保驾护航。

3. 伪基站识别技术

伪基站攻击存在一些通用性特征：比如手机在被伪基站攻击时，会出现正常信号的中断，伪基站发出的鉴权数据包也会和正常基站发出的存在某些差异，伪基站可能一次性在某个区域大量发出短信内容，通过大数据分析判断该区域有较多用户同时遭遇攻击，通过和电信部门的密切合作，让伪基站的判定更加准确。腾讯手机管家在手机端帮助用户拦截伪基站短信，安全大数据还可以通过这些数据，判断伪基站的大致位置，协助电信管理部门或公安机关抓捕伪基站犯罪人员等等。

腾讯麒麟伪基站实时定位系统实时发现诈骗短信，协助警方发现、抓捕伪基站犯罪团伙。当前，腾讯麒麟系统落地全国 20+城市，总体伪基站诈骗案发下降 70%。腾讯麒麟系统可实时精准定位伪基站地理位置，大大提高警方发现、抓捕伪基站犯罪团伙的效率，保护人民财产安全和企业声誉，对维护公共通讯秩序和安全意义重大。以深圳警方为例，使用腾讯麒麟系统 3 个月内，打掉团伙 13 个，抓获 110 人，缴获设备 59 套，车辆 43 台，降低伪基站发案率 74%，目前深圳市的伪基站已基本为零。

4. 服务端预警系统

腾讯神侦资金流查控系统用于阻断电信网络诈骗链条中，资金转移的关键环节。神侦由腾讯安全、北京市公安局及银行合作研发，可在案发前基于合作方提供的海量数据进行建模，通过机器学习快速分析出犯罪团伙手中恶意银行卡，同时追踪犯罪团伙的活

动区域以及资金转移路径等信息。这套基于海量数据建立的检测模型，能够及时协助警方和银行对诈骗资金进行冻结支付等处理。

腾讯灵鲲大数据金融安全平台依托腾讯近二十年的 QQ 黑产打击经验、AI 优势、腾讯安全反诈骗实验室首创的八维数据模型，以及世界一流的安全大数据团队等，已达到可对潜在金融风险企业全覆盖监测，全面、准确地描述风险详情，对金融风险预测准确率达到 99.9%。目前，灵鲲和国家工商总局、北京金融局、广州金融局和深圳金融办展开合作，接入了中国银行、招商银行、中信银行、京东金融等百余家银行、支付机构、互金机构、电商、O2O 平台。充分发挥大数据研判优势，在金融风险防范上取得了显著的成绩，每天预警的欺诈事件达数百万次，涉及资金规模超过 10 亿元。

四、防范互联网金融风险安全建议

1. 提升金融安全防范意识

互联网金融诈骗，跟传销组织较为相似，往往以高额利息为诱饵，吸引参与者投入资金。网民在选择理财产品时，首选要了解这个机构是否值得信任，是否为合法注册的公司机构，是否有国家认可的营业执照。通过工商注册机构查询互联网金融公司的经营资质鉴定真伪，就能有效降低风险。

此外，判断互联网金融机构的收益与风险说明是否合理至关重要。2015 年 9 月开始最高法划定了 24%和 36%的利率双线，低于 24%的部分为“司法保护区”，高于 36%的部分为“无效区”；而位于两线之间的为“自然债务区”，借款人有权拒付，但如果借款人自愿给付，则事后不得要求返还。在当前的市场环境上，收益率超过 10%的项目风险都极高，若无十足把握切勿轻信。

2. 安装安全软件实时开启防护

建议安装腾讯电脑管家等安全防护软件加强防护。腾讯电脑管家通过与深圳经侦的深入合作，能够对高风险投资平台进行直接拦截，防止用户上当被骗。此外，微信用户还可通过微信搜索小程序“灵鲲金融风险查询举报中心”，对可疑的风险平台状态进行查询，更好地保护自己和家人的财产安全。



深圳市公安局经济犯罪侦查局郑重提醒您：请守护好自己的“钱袋子”！

您要访问的网站：<http://www.tps138.com/?qqdrsign=02ce7>
已被监管部门预警，存在投资理财风险。

关闭网页

继续访问（不推荐）

您可以使用微信扫描下方二维码对风险网站进行举报和查询风险原因，
或访问[深圳市公安局网站](#)查询原因。



腾讯安全2018上半年互联网金融安全报告

数据来源：腾讯安全反诈骗实验室



腾讯安全联合实验室通过大量受害者信息及权威部门发布的公告信息，去主动发现、标记互联网金融诈骗组织，通过“灵鲲金融风险查询举报中心”微信小程序，向用户提供简单易用的查询入口。用户可以通过模糊搜索，去查询虚假互联网金融网站的相关信息，当用户发现可疑金融欺诈网站时，还可以通过小程序举报，再由专业安全工程师进行鉴别确认。



腾讯安全联合实验室

