【互联网与账户安全】工信部电信研究院袁琦：

互联网技术推动下的账户安全新思维

（本文选自微金融 50 人论坛演讲汇编系列之一：微金融的基础设施，独家推出，转载请注明出处）

互联网行业是一个创新的行业，它一直在思考如何创新、如何和各行各业进行融合。淘宝就是互联网和零售业的一个很好的结合；无人汽车是互联网正在改变汽车制造业的一大例证。同样，互联网也在改变金融业。传统金融行业也在随着技术的发展变化不断地前进。

一、互联网金融发展进程和现状

一方面，我国传统金融业的信息化发展的进程是一个金融互联网化的过程。从 1993 年的金桥金卡工程，到 95、98 年的网络银行、网络保险。从 97 年的中国各银行网站和网页，到保险信息网、证券网上交易系统。然后是 2013 年微信上出现的招商银行，包括 2010 年和 2012 年各大银行推出的智能手机客户端……随着技术手段的不断丰富，以及信息化的发展，金融业信息化的里程在不断地向前进。然而，传统的金融业由于垄断的性质而发展缓慢，只有在技术发展到非常成熟的时候才会向前进一步。

另一方面，互联网行业不断发展、迭代迅速、充满创新。国内外互联网金融发展的进程是一个互联网金融化的过程。这个过程的起源是 1998 年的易趣第三方支付，然后是阿里巴巴的支付宝、阿里小贷，以及众筹、比特币，再到各个公司推出的金融服务。这是一个从小额的支付到大额的货币开始进入互联网的过程，也是一个互联网向金融行业渗透的过程。

从以上两个方面可以发现，整个传统金融行业的互联网化的进程很慢。然而，互联网金融化是以一个核爆炸的过程在发展。

互联网金融的发展现状，总体来说是从跟随模仿向探索创新驱动转变。第三方支付、P2P 网贷等都是模仿国外的企业。中国的互联网企业在本土化改造过程中考虑了中国的国情，通过互联网思维方式考虑用户体验，跟随模仿的策略使其发展呈现良好态势。同时，阿里巴巴、京东、百度等具有代表性的中国互联网企业积极创新，在各自的平台上推出了金融服务。

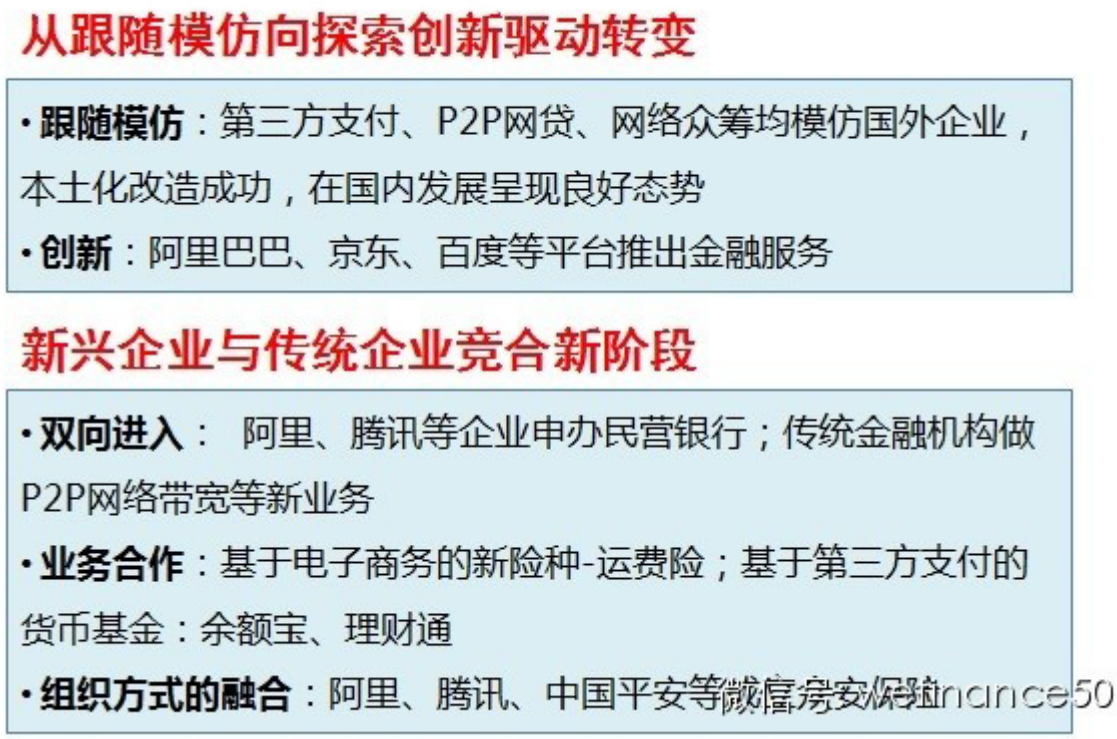

图 11-1 互联网金融发展现状

同样我们可以看到新兴的企业和传统的企业也在相互融合。各行各业的大佬应该思考在互联网技术发展下如何拥抱互联网，使自己的行业与互联网有更好的融合，从而改变整个经济的发展方式，以及传统产业的发展趋势。金融业中，新兴企业和传统企业存在双向进入的特征：阿里和腾讯在申办民营银行，传统的金融机构也在做 P2P 网络带宽等新业务。这些企业彼此之间也在进行一些业务合作和组织方式的融合：引入新险种（运费险）、余额宝和理财通等基于第三方支付的货币基金以及阿里、腾讯、中国平安等成立的众安保险。

二、账户支付安全是互联网金融的核心问题

互联网金融的新发展层出不穷，这也构成了互联网金融里面最根本的一个问题——账户支付的安全。无论是在传统的互联网行业，还是在新兴的互联网金融行业中，账户支付安全永远是一个基石，是一个核心问题。

1．支付安全问题是互联网金融的核心问题

互联网金融应用账户的表现形式有：银行账户、第三方支付、基金账户等。符合央行规定的聚集资金的账户有银行支付账户和第三方支付账户，其余所有的账户的资金都应该来自于这两类有央行牌照的账户。其中，银行支付账户的主体是银行企业，第三方支付账户的主体是第三方支付企业（例如支付宝、财付通）。

我们通过账户完成资金支付的整个生命周期流程。无论是银行支付的账户还是第三方，要完成交易则必须要经过这样的生命周期流程：账户开设，账户登陆，账户审核，账户资金转移和账户资金清结算。在这个流程中，银行和第三方并不相同：账户开设与登陆阶段，传统的金融业都是通过柜台进行操作，而第三方支付赋予用户线上操作的权限，账户审核是后台自动完成。因为第三方支付往往额度较小，所以其账户开设阶段的安全性尚可接受。并且在账户登陆、账户资金转移等阶段，整个安全性和以信息技术为基础的安全手段有关，所以账户安全贯穿账户完成资金交易的整个生命周期过程中，支付安全是互联网金融的核心问题。

2．互联网技术推动下的账户安全常见问题及安全威胁

道高一尺魔高一丈。关于账户安全问题，常见的有克隆网站、二维码应用、网络钓鱼、诈骗短信等等。它们的背后都是恶意软件和木马，这些恶意软件和木马会非法盗取账户和密码并诱骗用户转账或支付。

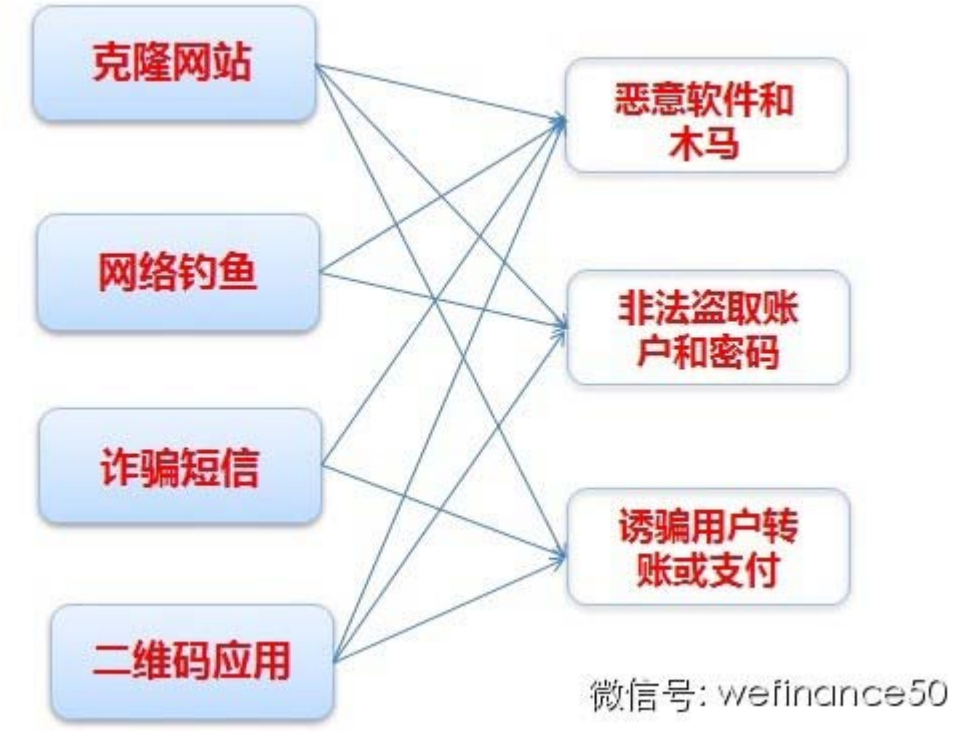

图 11-2 互联网技术推动下的账户安全常见问题

需要注意的是，账户安全并不只是涉及简单的账户。从互联网的角度，它与端（终端）、管（网络）、云（业务应用端）都有关。账户安全涉及的关键要素有：数据安全、应用安全、平台安全、网络安全、终端安全和用户安全。如果平台有了漏洞，黑客攻击到后台的平台，会导致一些资金损失；终端的软硬件的后门漏洞可能获取用户的支付信息；空中窃听用户的信息也可能导致账户受到安全威胁；用户存放账户的系统平台，以及用于业务结算的业务层也有可能获得一些信息；用户存在平台上的一些应用数据、用户数据、业务数据的损失，都有可能会对账户安全造成影响……账户安全需要保证用户的身份认证唯一、交易准确无误以及数据传输和存储安全，它将涉及端、管、云的每一个因素。

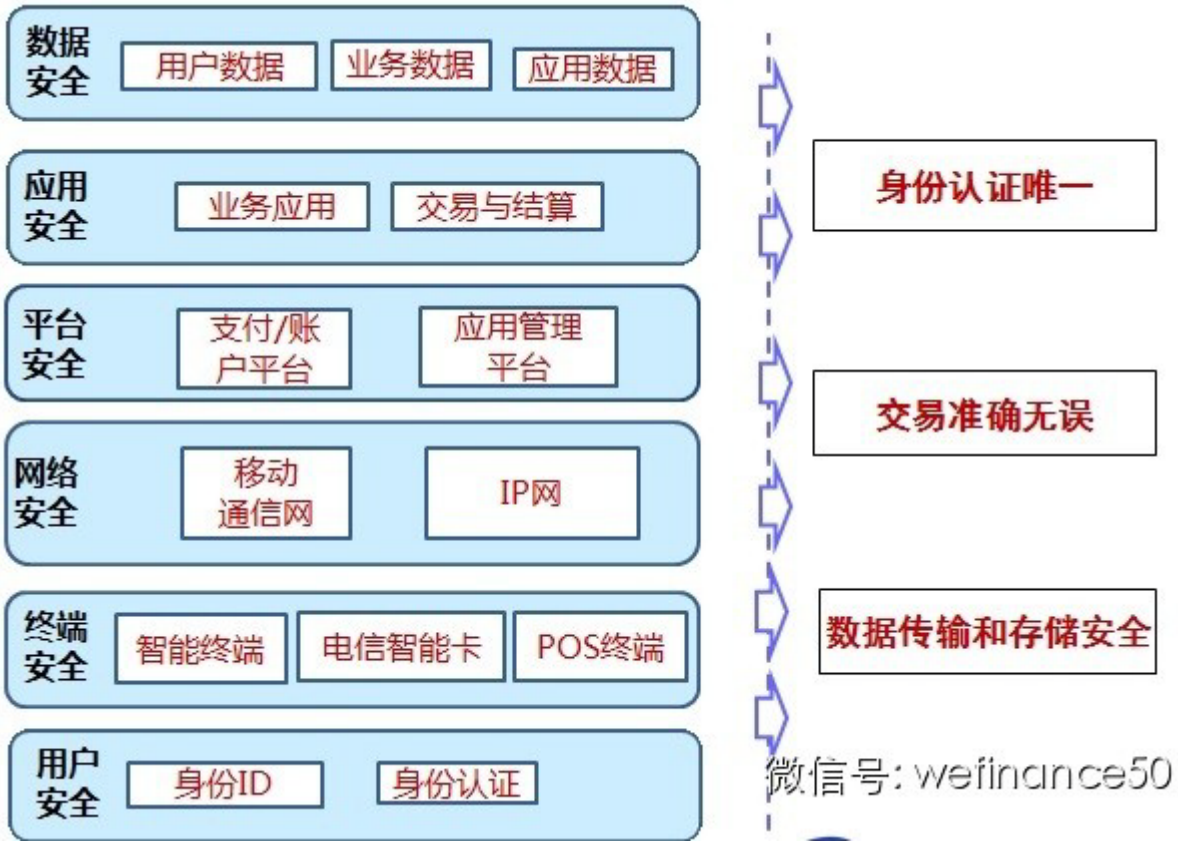

图 11-3 账户安全涉及的关键要素

相应的，账户安全面临的威胁也来自以上几个方面。在用户安全方面，一些用户登陆的账号、密码会被盗用或冒用；在终端安全方面，PC 和移动终端可能存在的病毒和恶意代码等都可能会导致用户信息泄露；网络安全威胁来自钓鱼和克隆网站；平台安全威胁是指部分业务存在从互联网入侵和控制的危险；数据安全就是交易账号和密码的盗用，以及保存的用户信息和交易信息存在泄露和滥用的风险。

3．账户安全技术解决方案

从账户安全的要素角度，账户安全技术解决方案有以下几个部分：身份认证要有多重的用户名和密码、U 盾、校验码、短信验证以保证用户安全；终端安全出现了一种技术，在终端划出一个可信区域，可信终端在可信区域使用支付应用、操作系统加固、应用软件安全检测、安装防病毒工具等；网络安全方面，通过网络安全防护和网络加密传输等保证账户安全；为了防止黑客攻击，可以对平台进行风险评估，并且采用一些安全防护的措施；客户端和服务器采用 SSL 加密、日志审计等保证应用安全；数据安全一般通过数据的加密、存储、传输和备份实现。目前，我们的支付领域常用的是账户安全的基础方案。不同的银行或者是不同的企业会将这些技术解决方案进行集成，从而更好地保证账户安全。

三、国内外账户支付安全监管政策和现状

1．国外账户支付安全监管政策

账户支付安全需要监管，不同的国家有各自的监管政策。韩国对所有从事支付业务的企业都实施强化准入条件的许可证制度并要求其接受金融监管委员会的监管，而且在保障交易和数据安全方面制定了明确的法律条文。这主要有三个方面，一是针对直接参与电子商务的公司出台了《电子商务消费者保护法案》和 2005 年颁布的增补条款（提供步骤以保护消费者的数据，确认支付结算的细节；在网站上提供服务供应商的完整信息）；二是要求所有从事交易的公司除接受监管外还要达到最低的安全标准，交易记录至少保留五年；三是市场运营商受到电信商业法案的规范管理，包含信息和数据保护的渠道。

日本的情况与韩国不同。日本是一个移动电子商务以及移动互联网比较发达的国家，其电子移动金融是发展最早也是最成熟的。这得益于日本宽松的金融管制政策，它允许运营商开展多种模式的支付业务，并且属于各个经济产业省管辖，央行则侧重对资金安全的管理。

欧盟的情况与韩国类似。欧盟委员会正式发布的《电子货币机构指令》覆盖已出现的大多数电子支付工具，包括卡基软件子钱包方案、充值卡、账户、互联网支付机制等，说明提供这类电子支付服务需要普通的银行执照或申请 ELMI 执照，这相当于准入资格监管。

在美国，非金融机构被允许开展电子支付业务。它的监管主要在各个州，大多受到货币转账等法律监管，有资本金、储备金和执照方面的限制，还会受到金融隐私、反洗钱等法律的约束。

2．我国账户支付安全监管现状

我国对非金融机构的监管起步较晚。2010 年，中国人民银行才出台了《非金融机构支付服务管理办法》，在此之前非金融机构都是监管的灰色地带。在 2010 年 12 月 1 日，中国人民银行颁布了《非金融机构支付服务管理办法实施细则》，使得各个企业的金融业务合法化。2014 年 3 月，中国人民银行发布了《支付机构互联网支付业务管理办法》和《中国人民银行关于手机支付业务发展的指导意见》征求意见稿，明确了交易和数据保护的要求。《管理办法》的第五章——《风险管理》中规定了信息和数据安全要求，《指导意见》的第三章——《保障信息与信息安全》规定了交易数据处理过程中的完整性、安全性和不可抵赖性，并要求对客户信息保密和防止信息泄露。另外，2013 年中国人民银行发布移动支付系列标准，对于移动支付从安全模块到网络传输和应用平台的整套方案都作出了技术要求。同时，工信部也发布了移动支付部分标准，包括总体安全、手机终端安全等要求。这些办法和标准为电子支付的安全提供了依据。

3．我国账户安全方面存在的问题

即便账户安全监管的各项政策在不断完善，账户安全问题仍在频繁发生。

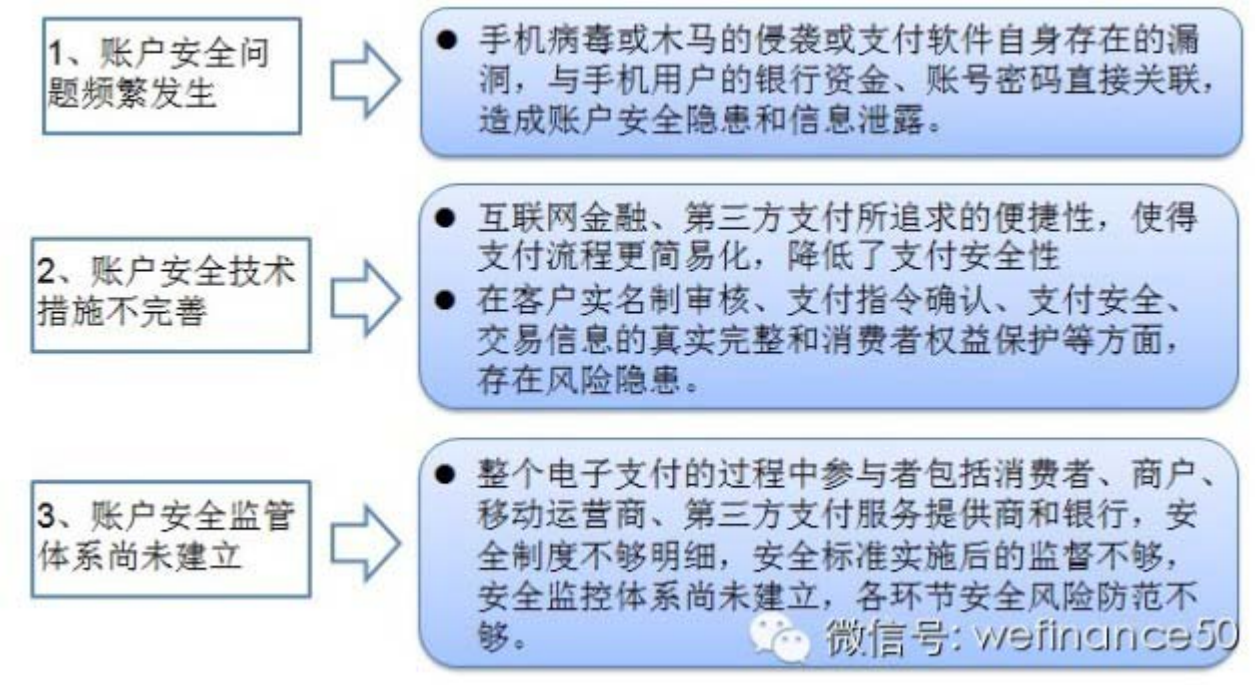

图 11-4 我国账户安全存在的问题

其直接原因是手机病毒或木马的侵袭或支付软件自身存在的漏洞，它们与手机用户的银行资金、账号密码直接关联，造成账户安全隐患和信息泄露。同时，账户安全技术措施不完善也是一个问题：互联网金融、第三方支付所追求的便捷性使得支付流程更简易化，也降低了支付安全性；在客户实名制审核、支付指令确认、支付安全、交易信息的真实完整和消费者权益保护等方面，存在风险隐患。此外，账户安全监管体系尚未建立。电子支付过程的参与者包括消费者、商户、移动运营商、第三方支付服务提供商和银行。针对这些对象和整个过程的安全制度不够明确，安全标准实施后的监督不够，安全监控体系尚未建立，各环节安全风险防范不够。

四、保障我国账户安全的建议

针对以上问题给出如下建议：

1．在政策方面，希望政府能够细化第三方支付和互联网金融账户安全方面的政策，并对账户、交易和数据安全保护的要求进行监督和实施。

2．技术方面，在终端、账户、业务交易等环节采用可信安全、加密和完整性等安全保护技术，通过手机号绑定、短信验证码等方式进行支付确认，保障通信安全；对业务和应用平台进行高等级的安全防护，防止恶意代码和病毒攻击；建立覆盖整个账户、业务交易环节的内部控制制度及实施监督机制，落实内部控制考核，确保账户、业务交易环节操作的规范性。

3．标准方面，希望尽快对账户安全标准进行监督和实施，开展安全标准的认证测试工作。

4．远期来看，应当积极开展对信用体系建设的探索，研究制定相应的交易规则，强化对交易双方的信用分析。同时，对已有的信用信息进行有效整合，实现部门间信用信息的共享，对失信的单位或个人及时纳入“黑名单”管理，并实现动态的发布以减少交易信息不对称，降低移动支付的信用风险。

不难发现，我国和国外最大的区别是国外拥有发达的信用体系和良好的信用机制，这是金融发展的基础和保障。因此，我国也应该建立这样的信用体系以促进金融业的蓬勃发展。