中国网络支付安全状况报告

（2012 年 10 月）

中国互联网络信息中心

目录

图目录

第一章 调查介绍

1.1 调查方法

1.1.1调查样本分布

电话调查的目标总体是中国大陆（除港、澳、台三地）网民。CNNIC 随机抽取华北、东北、华东、华南、华中、西北、西南 7 大区域内的 2300 个样本。调查样本根据城市所有电话局号，通过随机生成电话号码的方式，抽取住宅电话、小灵通、宿舍电话和手机进行访问。访问对象为最近半年有过网上支付行为的网民，成功样本 2300 个。具体样本分布见下表：

表 1 样本分布

城市	数量	城市	数量
北京	150	郑州	65
上海	150	成都	62
广州	150	重庆	62
深圳	150	昆明	61
杭州	100	贵阳	61
厦门	100	哈尔滨	60
苏州	100	长春	60
南京	100	天津	60
宁波	100	石家庄	60
扬州	75	沈阳	55
金华	73	佛山	52
西安	72	邯郸	30
兰州	72	洛阳	30
武汉	65	襄樊	30
长沙	65	岳阳	30

1.1.2调查时间

本次调查数据截止时间为2012年9月24日。

1.1.3调查方式

计算机辅助电话访问（CATI）。

1.1.4调查随机性和准确性控制办法

（1） 分别使用各个城市的所有局号（即电话号码的前四位）随机生成电话号码进行访

问。为防执行公司为了拨打的效率较高，只抽取部分使用频率较高的局号生成电话号码，造成样本的代表性有偏差，CNNIC采取由研究人员自己随机生成所有电话号码提供给执行公司。完成调查后，要求电话调查公司提供所有电话的拨打明细情况，进行抽查。

（2） 为避免上班族白天上班的影响造成的偏差，固话采取工作日晚上18:00以后、周末全天拨打电话的方法，手机采取全天拨打的方式。

（3） 为避免接通率对随机性的影响，对号码无法接通的情况，采取至少拨打三遍的方式。

（4） 为避免访员个人观点对访问造成影响，规定不需要读出的选项一律不加以任何提示，并追问到位。

（5） 电话调查结束后对数据进行了预处理、核对了变量的取值和变量之间的逻辑关系等，对于不合格样本予以整体删除处理。

1.2 术语界定

◇ 网民

指半年内上过网的中国居民。

◇ 网上支付/网络支付

网上支付是通过网上银行、第三方支付工具等进行货币支付或资金流转的服务，在本报告中也称“网络支付”。

◇ 网上支付用户

最近半年至少使用过一次网上支付这种网络应用的网民，在文中一些地方也简称为“用户”。

◇ 网上银行

网上银行是银行为客户提供的在线金融服务，包括开户、查询、对帐、行内转帐、跨行转账、信贷、网上证券、投资理财等。

◇ 手机支付

手机支付指手机网民使用其移动终端（手机）对所消费的商品或服务进行在线账务支付的方式。

◇ 网上支付安全风险

主要有三个层面：一是银行网站本身的安全性；二是交易信息在商家与银行之间传递的安全性；三是交易信息在消费者与银行/支付机构之间传递的安全性。本报告主要涉及最后一种，用户端使用的安全性，即用户在网络支付过程中存在的信息泄漏、交易欺诈等风险，造成用户权益受损。

◇ 第三方支付

指和国内外各大银行签约，并具备一定实力和信誉保障的第三方独立机构提供的交易支持平台。通过与银行的商业合作，以银行的支付结算功能为基础，向政府、企业、事业单位提供中立的、公正的面向其用户的个性化支付结算与增值服务。

◇ 钓鱼网站

仿冒真实网站的 URL 地址以及页面内容，骗取用户提交的银行帐号、密码等私密信息的网站。

◇ 地区划分标准

全国划分为七大区域。各区域包含省市如下：

华北地区：北京市、天津市、河北省、山西省、内蒙古自治区。

东北地区：辽宁省、吉林省、黑龙江省。

华东地区：上海市、江苏省、浙江省、安徽省、福建省、江西省、山东省。

华中地区：河南省、湖北省、湖南省。

华南地区：广东省、广西壮族自治区、海南省。

西南地区：重庆市、四川省、贵州省、云南省、西藏自治区。

西北地区：陕西省、甘肃省、青海省、宁夏回族自治区、新疆维吾尔族自治区。

1.3 调查摘要

◇ **第三方支付和网上银行支付并驾齐驱，快捷支付渗透近半用户。**我国网上支付用户最主要使用的网上支付类型是第三方支付账户余额支付和网上银行支付，分别覆盖了79.2%和 75.7%的支付用户。快捷支付和卡通支付也成为新的支付趋势，网民使用比例也达到了 40.4%。

◇ **支付宝用户覆盖优势明显，银联在线成长较快。**中国用户覆盖最广的第三方支付工具是支付宝，有 80%的网上支付用户使用支付宝实现网上支付，其在网民中的覆盖率遥遥领先于其他第三方支付工具。排在第二位的是财付通，有 21.1%的使用率；第三位的是银联在线，有 16.9%的使用率。

◇ **安全担忧成阻碍用户使用网上支付的重要原因。**30.4%的非网上支付用户是因为感觉不安全、担心资金被盗而不使用网上支付，还有 11.8%的非网上支付用户是担心账户信息泄漏。

◇ **用户安全意识不足，仅一半网上支付用户关注网上支付安全问题。**52.8%的网上支付用户关注网上支付的安全问题，还有 47.2%的用户对网上支付安全问题表示非常不关注或较不关注。此外，有 57.6%的用户表示不知道保障网上支付安全的办法。

◇ **用户对透露个人信息警惕性高，对即时通信链接防范意识不强。**当接到电话称退款，需要告知自己的姓名、账户或手机验证码信息时，只有 2.9%的用户愿意透露信息。当用户使用即时通信工具遇到对方发来的不明链接时，有 15%的用户会直接点击。

◇ **整体支付安全使用状况较好，仅 5.3%的网上支付用户认为网上支付不安全。网上支付**用户对网上支付安全性给予较高的评价，有 9.3%的**网上支付**用户认为网上支付非常安全，69.4%的**网上支付**用户认为网上支付比较安全，还有 16%的**网上支付**用户认为网上支付的安全水平一般。只有 5.3%的**网上支付**用户感觉网上支付不太安全或非常不安全。

◇ **大部分用户认为电脑支付安全性高于手机，安全感知受熟悉度影响较大。**60.9%的网上支付用户认为电脑支付比手机支付更安全，8.7%的用户认为手机支付更安全。15.7%的用户认为电脑和手机支付都很安全。

◇ **网上支付用户对担保交易支付安全性评价最高。**网上支付用户感觉安全性最高的支付服务类型是具有担保机制的第三方支付工具支付，有47.2%的选择比例；第二位的是普通网银支付，有 29.2%的选择比例；第三位的是具有赔付机制的第三方支付工具支付，即快捷支付，有14%的选择比例。

◇ **第三方支付企业中，网上支付用户对支付宝整体安全性评价最高。**在主要的第三方支付企业中，用户对支付宝整体安全性的评价最高，有92.1%的用户对支付宝的整体安全性给予肯定评价；第二位的是银联在线，有85.8%的比例；第三位的是财付通，整体安全评价比例为83.5%。从安全技术、安全产品感知、安全措施、问题解决和安全宣传五个维度进行分别评价，支付宝在大部分指标上评分都较为领先，在一些分类指标上，银联在线和财付通表现也较为突出。

◇ **网上支付用户遭遇支付不安全事件比例为3.2%，钓鱼网站诱骗支付占首位。**有3.2%的网上支付用户表示自己最近半年曾经遇到过支付不安全事件。用户遇到的最主要不安全问题是遭遇虚假网站欺骗后贸然支付，有64.4%的比例；第二位的是支付账号或密码被盗，有19.2%的比例；第三位的是支付过程遭遇木马病毒，有11%的比例；还有8.2%的用户遇到过个人资料泄漏的问题。

◇ **近一半用户遭遇支付安全问题时怕麻烦没有索赔。**遇到支付不安全事件的用户中，40%有实际的资金损失。在遇到不安全事件时，34.2%的用户是申请支付机构解决；9.6%的用户报警求助公安机关；有6.8%的用户自己找不法分子追偿。有41.1%的用户并没有追究责任，而是自己承担损失。其中有56.7%的用户没有追究支付不安全问题主要是因为觉得麻烦，费时费力；还有26.7%的用户觉得金额较小，无所谓；还有23.3%的用户不知道怎么解决。

第二章 网络支付发展概述

2.1 发展环境

互联网从娱乐向商务转变，支付成重要平台性应用

当前，世界正处于新一轮科技革命和产业革命的前夜，以互联网为代表的电子信息产业是当今世界发展的大趋势，也是推动经济社会变革的重要力量。中国互联网产业和应用呈现迅速发展势头，互联网“人口红利”持续释放支撑应用和产业持续增长，截至 2012 年 6 月，中国网民数量达到 5.38 亿，占世界网民数的四分之一，互联网普及率达到 39.9%。

中国互联网应用中娱乐功能一直非常突出，随着互联网发展阶段从量升到质变，商务类应用成为新的增长点。长期以来，网络游戏、网络音乐、网络视频成为带动中国网民增长和应用的重要推动应用，产业规模不断增长，成为引领中国互联网产业发展的领头产业。近年来，娱乐类应用在网民互联网生活中的重要性逐步降低，商务类应用呈现迅猛的发展势头，以网络购物、网上支付、网上银行为代表的交易类应用用户规模高速增长，在网民中的渗透率逐步上升，中国网民网络生活的重心已经由单纯信息获取、媒体娱乐转向商务等高级应用，中国互联网产业发展进入到了商务化阶段。

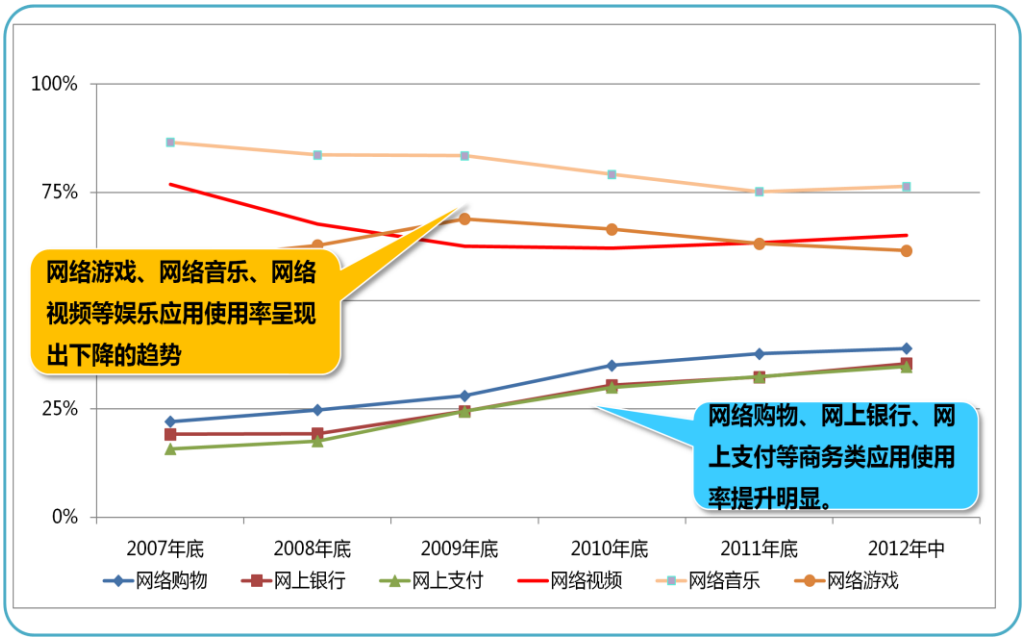


图 12007. 12-2012. 6 主要互联网应用渗透率变化

在传统经济社会，实现资金交付功能的银行等金融体系是市场运行的纽带；在网络经济时代，包括传统银行、第三方支付机构在内的线上支付服务体系形成关键性通路，是新经济时代的命脉。随着越来越多的衣食住行服务通过线上渠道进行资金的交付，网上支付已经成为支撑线上商务、零售、预订、教育医疗等的综合服务平台。第三方支付企业，特别是线上第三方支付企业将先进的信息技术与支付服务充分结合，弥补了传统商业银行在线上资金处理效率、信息流整合以及个性化服务等方面的不足，成为网络经济时代金融服务体系日益重要的组成部分。

2.2 市场容量

网络零售和本地消费服务激增，支付市场蕴含巨大空间

随着中国网络零售市场的迅猛发展，线上消费的生活服务类型不断拓宽，交易规模持续增大，网上支付蕴含巨大的市场空间。2007-2010 年，中国网络零售市场交易规模增长近 10 倍，从 542 亿元增长到 5231 亿元人民币。2011 年依然保持 44.6%的增长幅度，全年交易规模达到 7566 亿元，网络零售市场交易总额占社会消费品零售总额的已经达到 4.2%。据波士顿咨询公司预测，至 2015 年，我国网络零售市场将达到 2 万亿元人民币以上，超过美国；人均网上消费额将达到 6220 元人民币，超过美国目前 1000 美元的平均水平。

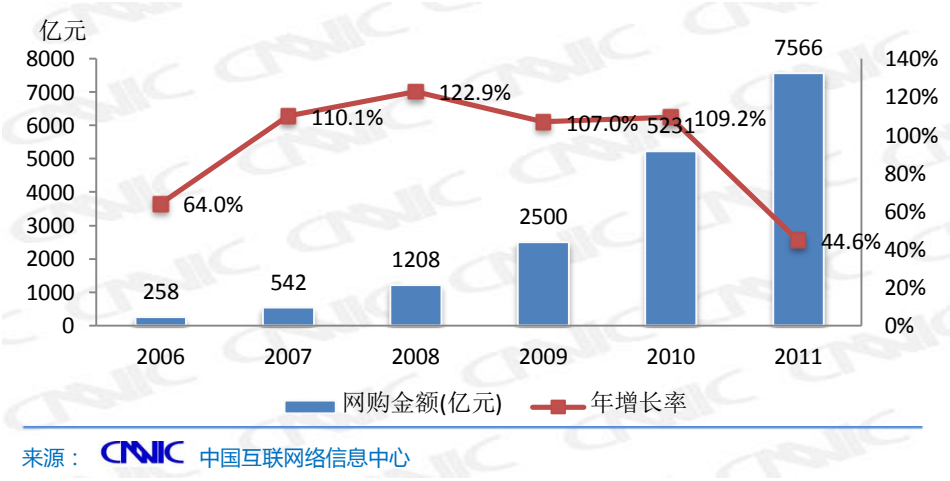


图 22006-2011 年中国网购交易金额及增长率

表 22011 年网络零售交易额中美对比

	美国	中国
网络零售交易额（人民币，亿元）	15465	7566
网络零售交易额增速	16.2%	44.6%

占社会总零售额的比例	4.6%	4.2%
人均网络购物交易额（人民币，元）	6500	3901

数据来源：CNNIC、美国普查局[1]、波士顿咨询公司

中国网上交易的需求持续增长，而网上支付应用发展的基础条件却落后于美国。美国的网上支付是从发展成熟的线下信用卡体系延伸到互联网的，信用卡和银行支票已经成为较为普及的支付方式。而我国一方面线下信用体制不够完善，另一方面银行卡支付系统建设时间也较短。互联网的快速发展使得对支付的需求远远快于支付基础水平，这些都推动了网上支付持续快读发展。当前，民营第三方支付企业已正式纳入央行的金融机构管辖范围，第三方支付本身的身份问题也得到圆满解决，金融风险大大降低，进入“正规军”的第三方支付企业将迎来更为迅猛的发展。

2.3 用户规模

网上支付用户不到四成网民，未来增长趋势良好

近年来，以网上支付为代表的商务类应用持续快速增长，并引领其他互联网应用发展，成为中国互联网发展的突出特点。近年来，网上支付用户规模连续保持高速增长，成为引领各类互联网服务增长的代表性应用。

截至 2012 年 6 月，中国使用网上支付的用户规模达到 1.87 亿人，在网民中的渗透率为 34.8%。2008-2011 年用户增长了 3.2 倍，年均增长 47.5%，是用户年均增长最快的互联网应用之一。

[1]美国普查局. 零售额和网络零售额季度估算（2011 年第四季度）. http://www.census.gov/retail/, 2012.3.26

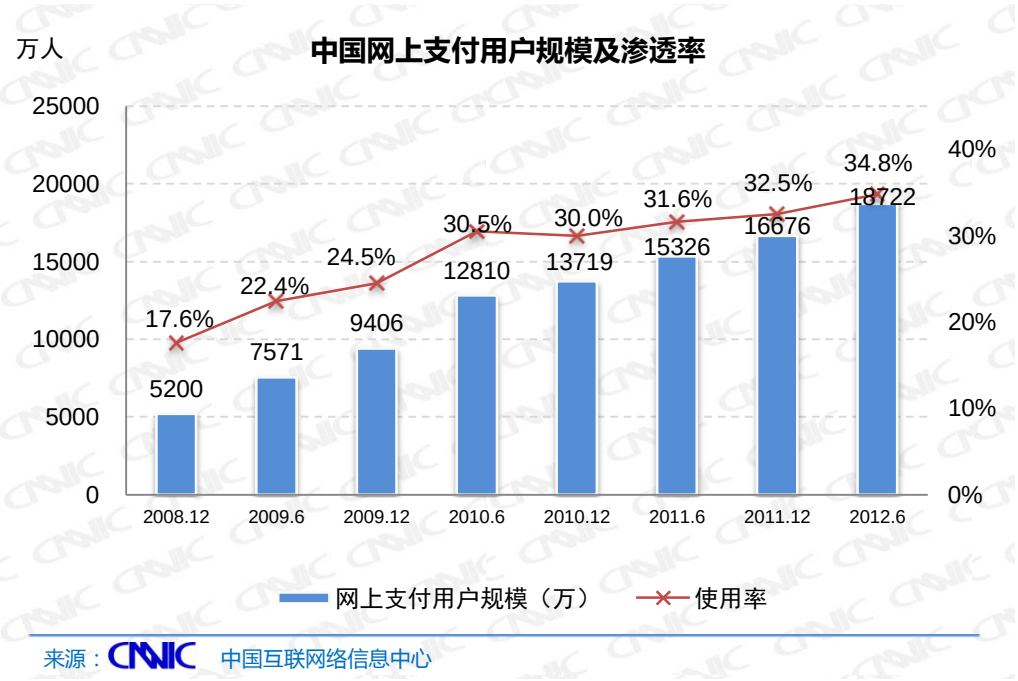


图 3 中国网上支付用户规模及渗透率

与国外发达国家相比，我国未来网上金融用户和市场增长空间巨大。以网上银行为例，2010 年美国网上支付用户占全国网民的比例为 58%[2]。而截至 2012 年 6 月，中国的网上银行渗透率仅为 35.5%。对比中美两国不同年龄段的用户网上银行渗透率发现，中国各个年龄段网民网上银行普及率也均低于美国相应群体 20 个百分点以上，尤其是中年群体差距更为突出，34-45 岁、46-55 岁和 56-65 岁的网民使用网上银行的渗透率差距分别为 27.3，28.6 和 37 个百分点。

[2]数据来源：PEW　http://www.pewinternet.org/

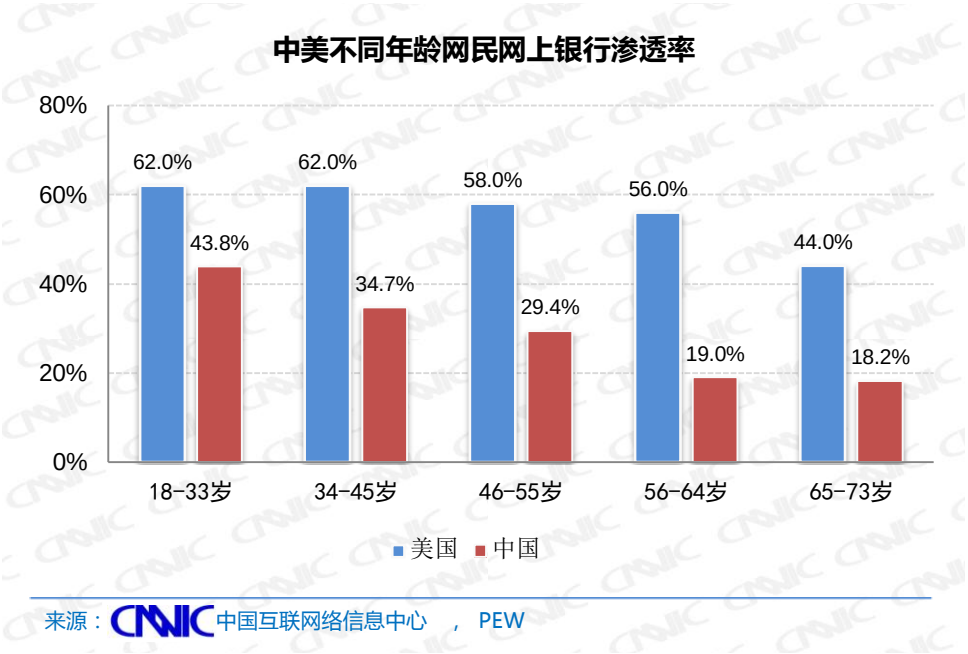


图 4 中美不同年龄网民网上银行渗透率[3]

我国网上金融的增长还远远没有触顶，尤其是对于将成为未来网民增长重要群体的中年人群，还有较大的渗透空间。从未来发展的预期看，我国互联网渗透逐步加深的势头不可逆转，网络消费供需面持续积极向好，这些都将推动网上银行、网上支付应用人群在未来较长时间实现较为稳健的增长。

[3]美国数据来源于 PEW：Generations 2010。中国数据来源于 CNNIC。

第三章 网络支付安全生态发展

3.1 网络支付安全风险及重要性

3.1.1 安全性关乎网络支付命脉

保密性、完整性和可识别性是保障网上支付安全的三大因素

风险是经济金融活动的共有属性，防范风险、保障安全就成为支付系统运行的基础要素。支付体系运行过程中潜在的风险主要包括信用风险、流动性风险、法律风险、运营风险、系统性风险等。在用户使用层面，业界普遍认为网上支付的安全性因素主要体现在以下三个特征上：

一是信息的保密性（confidentiality），能够保证信息不会泄露给非授权的主体，只有授权用户才能访问系统中的信息，而限制其他人对计算机信息的访问。保密性包括网络传输中的保密和信息存储保密等方面，保证支付信息与支付系统不被非授权者获取或利用。

二是数据完整性（Integrity），保证支付信息与支付系统真实、准确、数据的一致性，防止信息的非法修改。包括身份真实、数据完整和系统完整等方面。

三是身份的可识别性（validation）。能够鉴别通信主体身份的真实性，保证交易双方的身份可以识别和确认，未授权的用户不能进行交易，并且不会拒绝合法主体对系统资源的正当使用。

从支付安全的发展现状来看，分析用户网上支付主要出现的安全问题，由技术系统导致的风险相对较少，更多的问题主要集中在相对缺乏防御技术保障的用户端层面。如被钓鱼网站欺骗，受木马程序窃取密码、虚假银行网站套取用户信息的等等，破坏了信息的保密性、数据的完整性和身份的可识别性，从而产生相应的安全问题。

3.1.2 网民对支付安全诉求强烈

用户对支付安全性的诉求强烈，与便捷性并驾齐驱成为用户最关注的因素。

随着支付服务在网民生活中的加速渗透，方便安全已经成为决定用户支付工具选择的核心因素。调查显示，用户选择支付平台最关注的因素是支付过程便捷性和支付安全性，分别有 57.7%和 51.5%的选择比例，远远超过排在第三、四位的有折扣或积分活动、品牌形象。

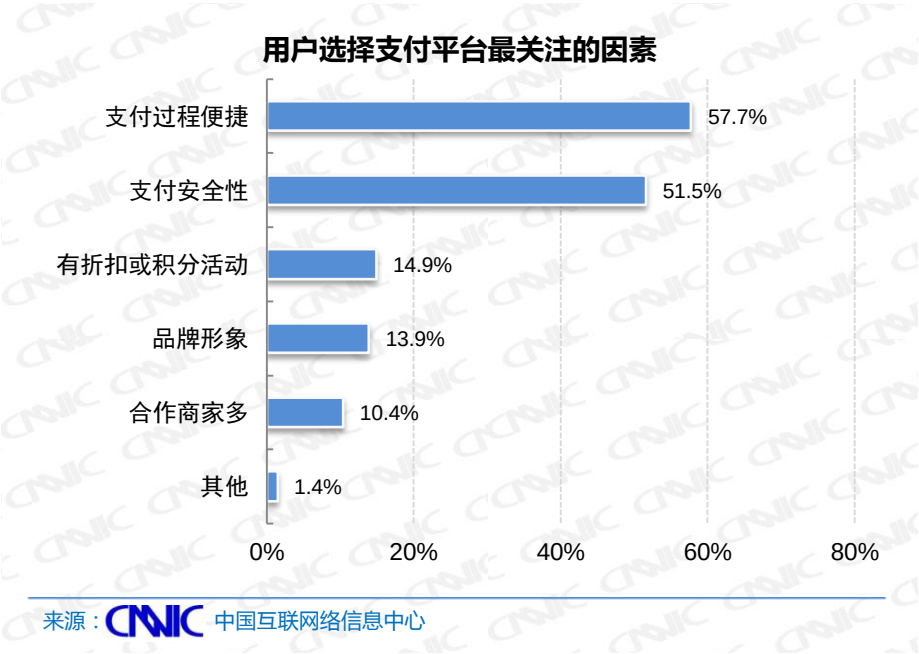


图 5 支付用户选择支付平台最关注的因素

安全担忧成为制约非网上支付用户使用网上支付工具的重要障碍。不使用网上支付的网民中，有 43.5%的是因为不需要网上支付工具，这部分人群的网络生活还没有从娱乐过渡到商务阶段，还处于网络应用的较浅层。此外，有 30.4%的用户是感觉不安全、担心资金被盗而不使用网上支付，还有 11.8%的用户担心账户信息泄漏。出于安全性的考虑，尤其是资金和信息安全的担忧成为阻碍用户使用网上支付的重要障碍。

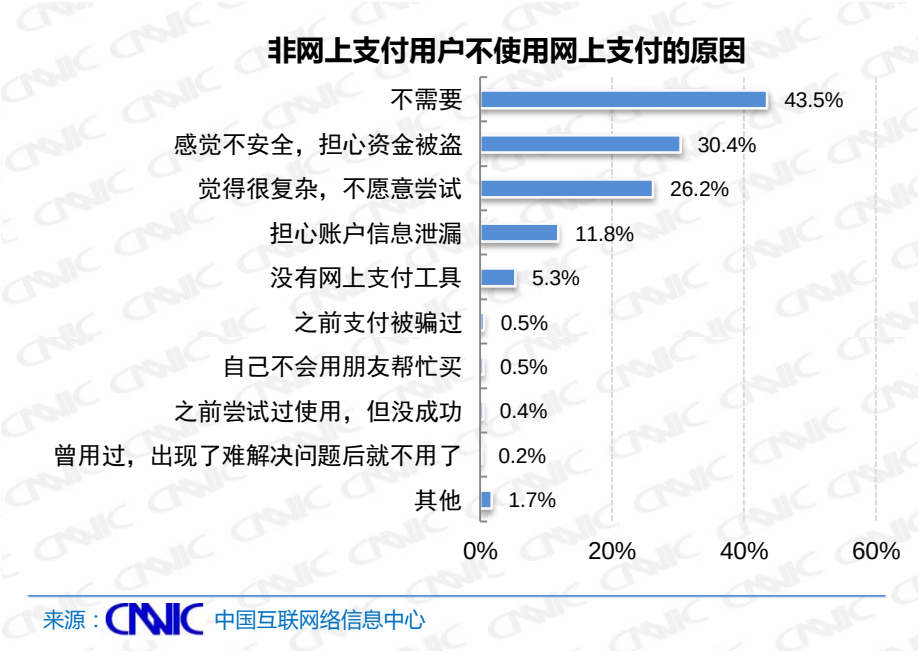


图 6 非网上支付用户不使用网上支付的原因

3.2 产品发展与安全措施并行

3.2.1 移动化、社交化支付安全风险增大

移动化浪潮下，移动支付将呈现迅猛发展的势头。据 Gartner 预测，2012 年全球移动支付用户数量将达到 2.1 亿人，同比增长 31.3%；2012 年全球移动支付交易规模预计将达到 1715 亿美元，较 2011 年增长 61.9%。移动互联网迅速发展和社交化应用的加深渗透，对网上支付的应用发展也产生巨大影响，但在便利和丰富用户线上生活的同时，也带来了一些新的风险。

一方面，移动支付作为新的支付手段发展异常迅速，移动支付系统结构多样化，参与的主体众多。多样化的系统结构和众多角色参与，使得安全风险必然随之增加。此外由于体积小、携带方便更容易被窃或丢失，移动支付的移动性也使其安全保障的难度加大。另一方面，社会化应用网站上的第三方应用程序使犯罪分子的作案工具发生了迅速变化，用户更容易受到攻击。网络犯罪分子往往利用朋友之间的信任，诱使用户点击原本会防范的链接。如微博上使用缩略网址更容易掩盖恶意网址并将用户引向这些网址。未来越来越多的网络犯罪分子将在最流行的社交网站上利用此类手法，会增大处于快速发展中的网上支付使用风险。

3.2.2 企业产品创新与安全性提升

第三方支付机构和银行纷纷从安全技术、产品功能、综合保障、业内合作等方面通过加强新技术应用，开展产品功能创新，完善综合保障，全面应对网上支付的新老安全风险。

首先，在安全技术层面，面对目前移动支付过程中存在的安全隐患，如恶意推广类手机病毒、隐私窃取类手机病毒、自费消耗类病毒问题，HTML5 技术能减少网页的跳转，有效地降低钓鱼网站和病毒的危害，被第三方支付机构广泛推行。支付宝采用了 HTTPS、私有安全算法、密钥定期更新、硬件识别码、订单签名等领先的安全技术。财付通推行了移动支付 HTML5 技术，在 QQ 团购、QQ 电影票、QQ 酒店等多项腾讯重点业务产品和服务中已率先支持。

其二，在综合保障方面，支付宝提供了身份认证、定制支付方式、安全传输、密钥定期更新等方式来确保用户账户安全。通过不同额度分类支付方式兼顾便利与安全性。一旦手机丢失，用户可以联系支付宝客服帮助监管冻结支付宝账户，也可以在电脑上操作，登录账户以后关闭无线支付总开关。在遗失手机的时候也能远程解除对设备的授权，第一时间保障资金安全。此外，支付宝还与微软强强联手，就共同开发和部署“设备健康模型”展开合作，

有望使网上支付的安全保护进入到一个更智能、更聪明的新阶段。

其三，在安全合作方面，财付通用户可在 QQ、UC 等手机浏览器上，直接使用财付通 HTML5 支付，省去下载、安装和更新移动支付插件的麻烦。中国银联与 UC 推出基于 UC 浏览器的银联移动安全支付解决方案，采取了浏览与支付分离的技术架构。浏览网页的安全交给 PC 浏览器，支付安全交给银联安全支付插件。银联支付插件通过与银行服务器直接对接，采用 3DES 和 1024 位的 RSA 算法验证和加密技术，使用银行级别的 HTTPS 加密通道进行数据传输。

3.3 支付安全生态环境发展

3.3.1 支付安全政策环境尚未建全

网络支付涉及到网络安全技术、数字签名技术、民事责任分担机制、第三方交易平台等相关问题，因此网络支付的安全性离不开众多配套法律的完善。我国陆续出台《中华人民共和国电子签名法》、《电子支付指引（第一号）》等，分别从法律上确定了电子签名的合法地位，并对网上交易的安全性提出了指导性要求，为网络支付安全提供了基础保障。近年来主管部门通过加强了对网上支付的管理，出台《非金融机构支付服务管理办法》及实施细则、《支付机构反洗钱和反恐怖融资管理办法》、《支付机构预付卡业务管理办法》，对非金融机构开展支务实施了相应的金融管制要求。在规范经营方面，要求支付机构应按核准范围从事支付业务、报备与披露业务收费情况，制定并披露服务协议，核对客户身份信息，保守客户商业秘密等。在资金安全方面，主要强调支付机构应在同一商业银行专户存放接收的客户备付金，且只能根据客户的指令划拨等。网上支付安全保障的法律环境在不断优化。

虽然有现行的法律法规对网上支付主体、经营机构进行规范，但针对网上支付的综合安全保障方面，还缺乏综合性的法规来明确银行、商户等相关方面责任义务；针对用户支付安全问题的追偿也缺乏明确的监管主体，来有效保障用户财产和信息安全。西方发达国家如美国和欧盟，多是沿用现有传统银行和支付管理法律来监管线上支付，由银行主要承担了保障网络安全的责任。而国内的银行发展滞后于国外，信用体系尚未完善，因此无法完全沿用线下管理体系来规范线上支付行为，使得线上支付安全的政策法律环境出现诸多监管空缺。与国外相比，我国支付业务监管还可以有进一步完善的空间，特别是普通用户的保障机制，以及安全利益相关方在安全方面的权责界限权责界定方面，亟需进一步明确化。

3.3.2 支付企业风险管理机制革新

支付企业完善技术手段保障用户安全

目前主要第三方支付企业采取了较多技术手段保障用户网上支付的安全，安全产品保护体系包括 OTP 和 PKI 体系。OTP 体系主要包括手机动态口令技术和宝令技术。PKI 体系主要包括数字证书和支付盾技术。两大体系从技术层面保障用户支付安全。

表 3 支付企业使用的部分安全支付技术手段

安全技术	实现方式及功能	安全级别
支付盾技术	以物理介质存在的数字证书	★★★★★
数字证书	绑定了公钥及其持有者的真实身份（若拥有实名认证机制，则同等于五星安全级别）	★★★★☆
宝令技术	独立的物理介质，随机显示密码（若拥有实名认证机制，则同等于五星安全级别）	★★★★☆
手机动态口令技术	向绑定手机发送随机产生的动态密码，无密码不能支付	★★★

联盟合作、统一标准，提升支付安全保障性

2011 年，在监管部门的指导下，由支付宝发起，联合第三方支付公司、银行、安全厂商、浏览器厂商及商户伙伴成立“安全支付联盟”，联盟包括了支付产业链上的所有环节，涵盖传统及无线应用场景。2012 年 5 月，支付宝与国内领先的 9 家第三方支付公司联合发起组建了第三方支付安全合作联盟。第三方支付企业将充分发挥整体效应，通过共享行业信息，共御行业风险；在信息共享基础上，合作探索更多层面、更丰富手段的联防机制，建立更加健康有序的行业安全经营环境。2012 年 9 月，支付宝牵头成立国内首个互联网商户安全联盟，美团、大众点评、汇元网等多家电商加盟，这意味着电子商务产业安全阵线的进一步完善。联盟将通过开放联防标准，配合安全技术、防控方案和安全产品，帮助电商防御传统的木马、钓鱼安全威胁。联盟重点对用户资料泄露所引起的安全风险进行联防布控，通过联合安全防护，电商由于用户账户、银行卡信息被盗引发的支付安全风险案

件量，以及支付资金损失均可以下降 90%左右。仅 2012 年上半年，支付宝就与合作伙伴联手屏蔽了超过 13.3 万个针对网购领域的钓鱼网站，平均每周屏蔽钓鱼网站量超过 5000 个。庞大的反钓鱼信息库和成熟的联防共享机制，有效防范了用户损失。

为了建立统一的业界标准，最大程度的降低支付卡风险，支付卡行业数据安全标准委员会 PCISSC 联合制定了旨在严格控制数据存储以保障支付卡用户在线交易安全的数据安全标准，即 PCI-DSS 安全认证标准。它不仅是全球信用卡支付必须的认证标准，也为各机构提供了一个最高级别的保障敏感信息安全性的产业工具和方法的通用集合。国内大多数第三方支付企业也申请了 PCI-DSS 认证，一些第三方支付网关构已经通过了 PCI-DSS 数据安全标准的合规认证，如快钱、支付宝等。第三方支付的参与和努力将有助于电子支付的安全体系的构建。2012 年 8 月，中国移动和中国银联正式签署合作协议，确定手机移动支付的统一标准。统一移动支付标准有利于提高金融安全，减少因手机移动支付系统标准差异造成的风险漏洞。

3.3.3 相关方在安全领域期待深度合作

网上支付安全问题不仅涉及第三方支付机构，还与整个支付生态产业链上的银行、商户、安全厂商以及监管部门紧密相关。随着安全问题在支付行业发展过程中的重要性进一步凸显，第三方支付企业联合支付生态链上下游企业进行安全合作，成立支付联盟、统一安全标准、联合开展防护，为保护支付安全运行起到了积极的促进作用。未来银行、第三方支付机构、商户需要加强深入的合作，进一步深化各方协调与合作，提高整体应对支付风险的能力和水平。只有支付生态链的各方参与者深度合作，在保障支付安全上形成闭环，才能为用户提供更严密的安全保障。

3.3.4 用户支付安全意识及技能亟需加强

用户安全意识不足，仅一半用户关注网上支付安全问题。对安全问题关注度一方面与整体安全水平有关，另一方面受用户对安全性的敏感程度影响。调查显示 52.8%的网上支付用户关注网上支付的安全问题，还有 47.3%的用户对网上支付安全问题表示非常不关注或较不关注。

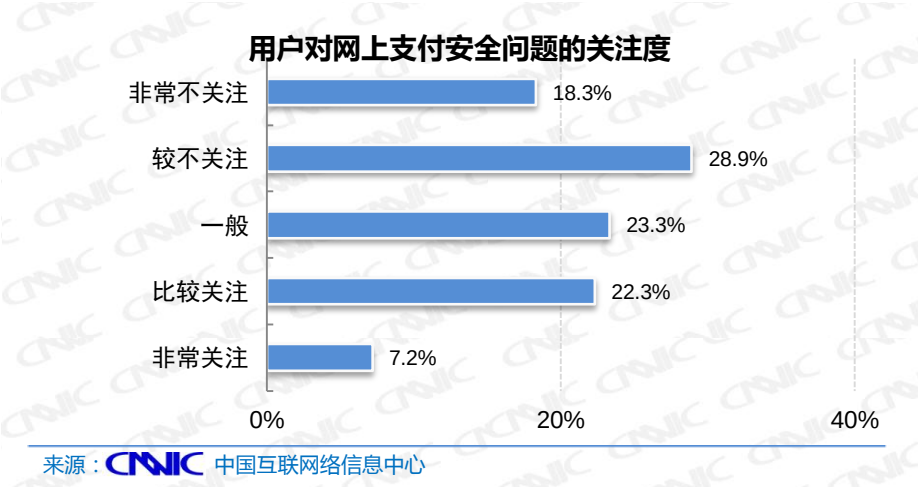


图 7 用户对网上支付安全问题的关注度

有 49.2%的用户表示听说过网上支付的不安全事件，最主要的是钓鱼网站和帐号、密码被盗情况。其中有 45.8%的用户听说过“虚假网站欺骗后贸然支付”，有 43.6%的用户听说过“支付帐号或密码被盗”。

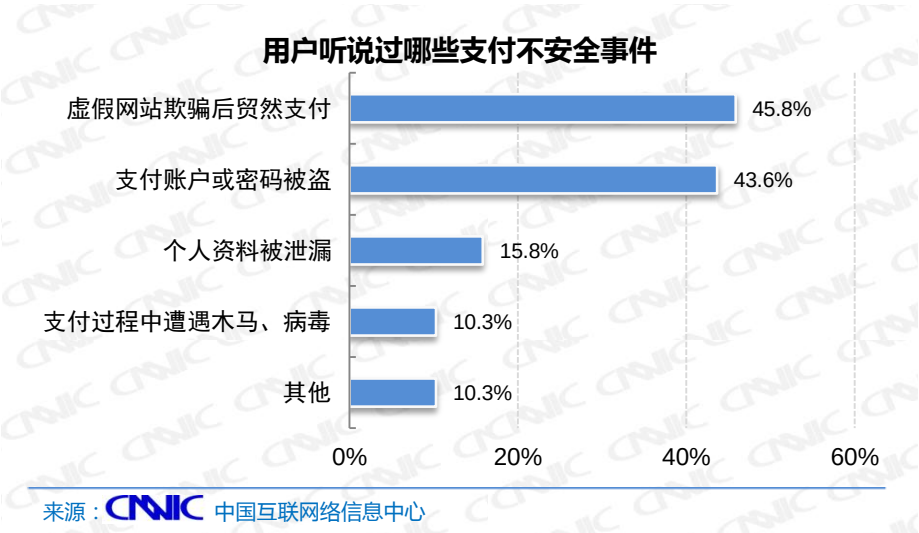


图 8 用户听说过哪些支付不安全事件

只有 42.4%的用户表示知道保障网上支付安全的办法。在不提示的情况下，支付用户表示了解最多的保障支付安全的方式是电脑杀毒和防火墙（30.8%）；表示知道使用动态密码、动态口令卡的有 30.6%；知道设置强安全密码的有 29.9%。

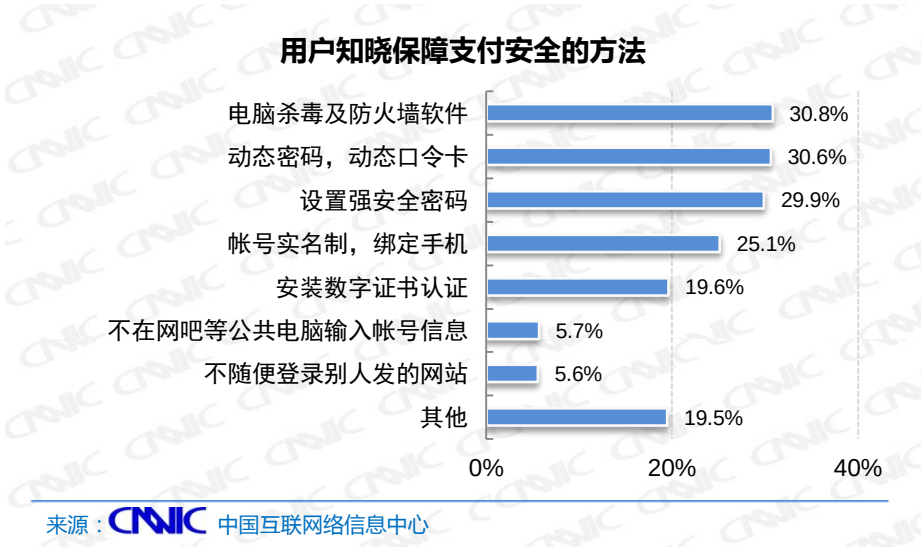


图 9 用户知晓保障支付安全的方法

第四章 用户安全感知及安全问题

4.1 用户支付使用行为

第三方支付和网上银行支付并驾齐驱，快捷支付渗透近半用户。

我国网上支付用户最主要使用的网上支付类型是第三方支付账户余额支付和网上银行支付，分别覆盖了 79.2%和 75.7%的支付用户。快捷支付和卡通支付也成为新的支付使用趋势，使用率也达到了 40.4%。

快捷支付功能具有里程碑的意义，其降低了网上支付的门槛，同时也提高了安全保障性。以支付宝为例，用户第一次签约认证时，需要做双向网络认证，一是通过互联网与银行实时信息的认证；另外针对金额较大的交易，支付宝还会通过人工回呼用户的方式，确认是否其本人进行操作。如果确认非本人操作，可以及时截留资金并退回银行卡。此外，支付宝还建立了 72 小时赔付机制，如果用户否认交易并通过支付宝客服以及风险管理体系确认，在用户提供了相关证明后，支付宝会在 72 小时内全额赔付。

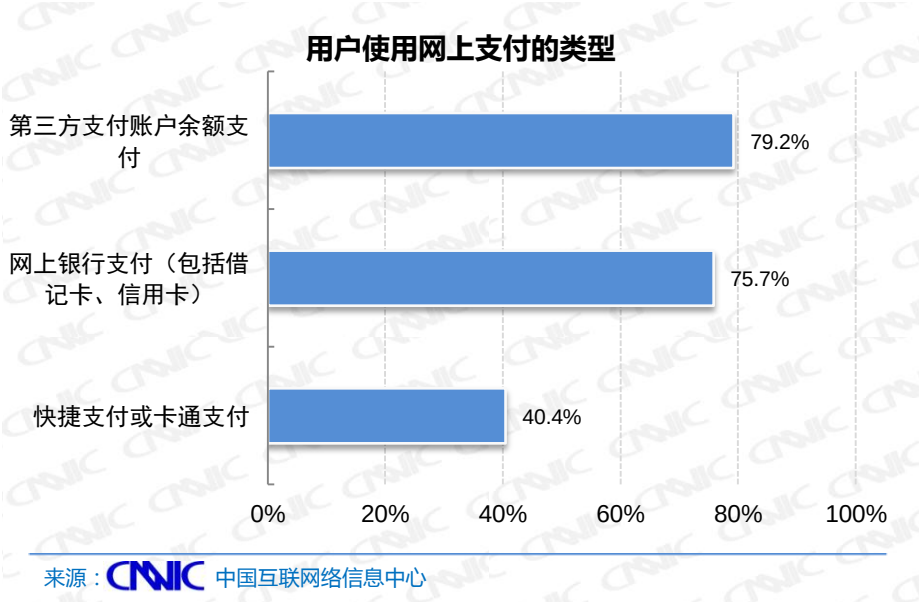


图 10 用户使用网站支付的类型

移动支付呈现快速发展的态势，支付宝、财付通、快钱、汇付天下等互联网支付厂商纷纷推出移动支付产品，进行了大规模的市场推广活动；移动、联通和电信三大运营商也纷纷成立支付公司，移动近场支付商用城市不断增加。手机网上支付用户规模达到 4426 万。手

机支付作为未来的发展趋势，目前依然处于成长期，未来手机支付将向多平台应用发展，与二维码、LBS 技术的结合，支付的形式和场景将更加多样化。

支付宝用户覆盖优势明显，银联在线成长较快

用户覆盖最广的第三方支付工具是支付宝，有 80%的网上支付用户使用支付宝实现网上支付，在网民中的覆盖率遥遥领先于其他第三方支付工具。排在第二位的是财付通，有 21.1%的使用率；第三位的是银联在线，有 16.9%的使用率。

支付宝由于早期依托于阿里巴巴和淘宝网，用户渗透基础较好，已经成为支付行业的标杆企业。腾讯旗下的财付通受拍拍网的影响，也有相当规模的用户覆盖。银联在线自 2011 年发展在线支付业务以来成长迅速，是最近一年成长较快的第三方支付企业。

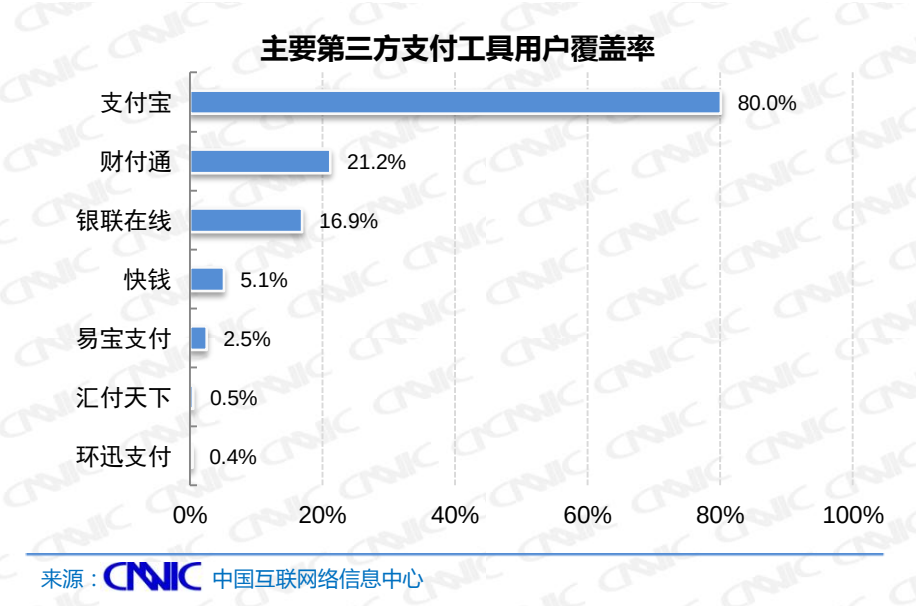


图 11 主要第三方支付工具用户覆盖率

部分网上支付用户进入频繁支付时代

有 43.1%的用户使用网上支付的频次依据具体情况而定，部分群体的网上消费行为相对较不密集。但是，有 11.6%的在线支付用户每周在线支付多次，10.7%的用户每周在线支付一次，这部分群体已经将网购、预订、充值、诸多生活服务等消费过程都通过在线支付手段实现。

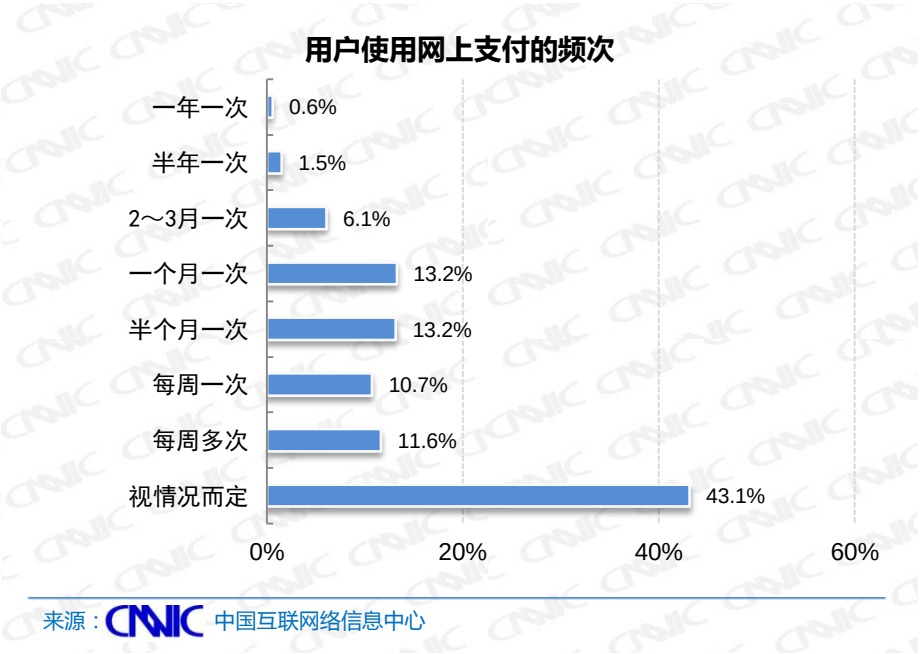


图 12 用户使用网上支付的频次

4.2 用户支付使用安全感

中国普通网民对支付安全担忧较少。与日本网民对支付安全性的担忧较为强烈不同，中国网民对支付安全性的担忧相对较少，只有 2%和 7.7%的中国网民表示在自己网上支付或网购时对信用卡或银行卡安全性很担心或者极其担心；有 46.5%的用户表示有一点担心，有 43.4%的中国网民表示一点也不担心，这一水平与美国、波兰、瑞典等互联网发达国家较为相似。

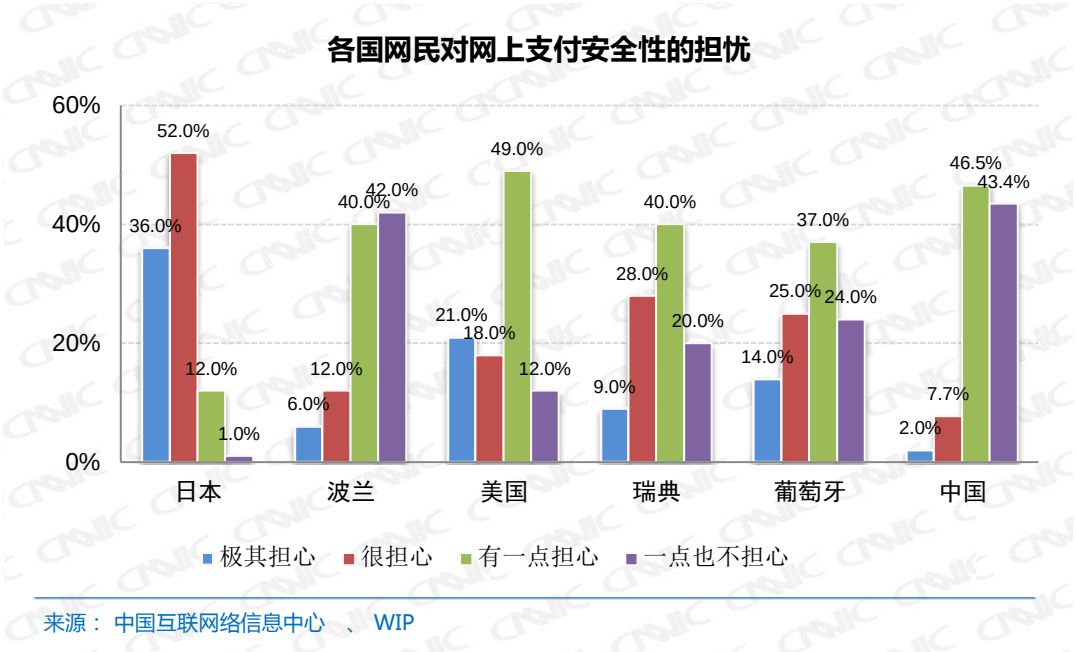


图 13 各国网民对网上支付安全性的担忧

支付安全性使用状况较好，仅 5.3%的网上支付用户给予网上支付安全评价

用户对网上支付安全性给予较高的评价，有 9.3%的**网上支付**用户认为网上支付非常安全，69.4%的**网上支付**用户认为网上支付比较安全，还有 16%的**网上支付**用户认为网上支付的安全水平一般。只有 5.3%的**网上支付**用户感觉网上支付不太安全或非常不安全。

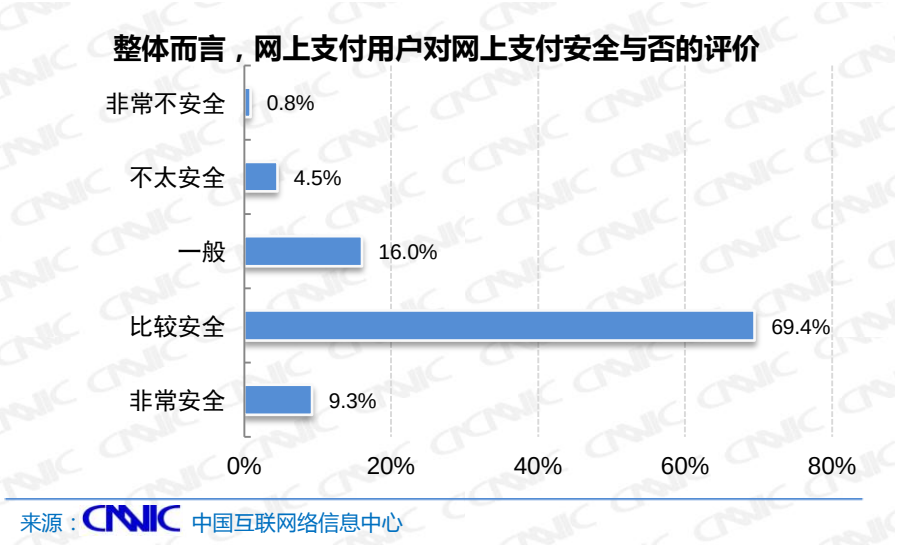


图 14 整体而言，网上支付用户对网上支付安全与否的评价

针对网上支付的不安全因素，用户认为首要提升的是技术防护手段（45.3%的选择比例），

此外，相关政策法规（40%）、安全保障机制（38.3%）和用户安全意识（36.3%）都是较多用户认为最需要提升的方面。用户对企业安全产品相对较为满意，只有 18.6%的用户认为企业安全产品是最需要改善的因素。

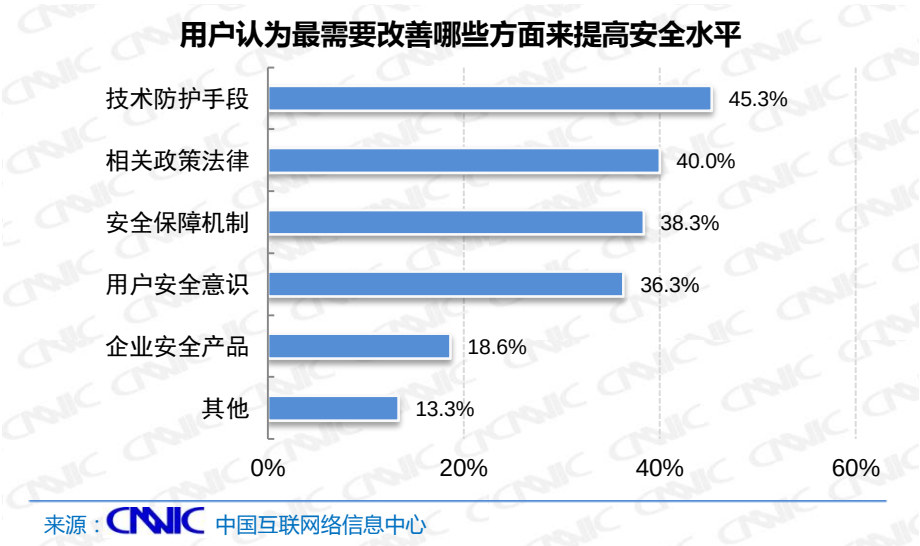


图 15 用户认为最需要改善哪些方面来提高安全水平

大部分网上支付用户认为电脑支付安全性高于手机，安全感知受熟悉度影响较大

有 60.9%的网上支付用户认为电脑支付比手机支付更安全，8.7%的用户认为手机支付更安全。15.7%的用户认为电脑和手机支付都很安全。

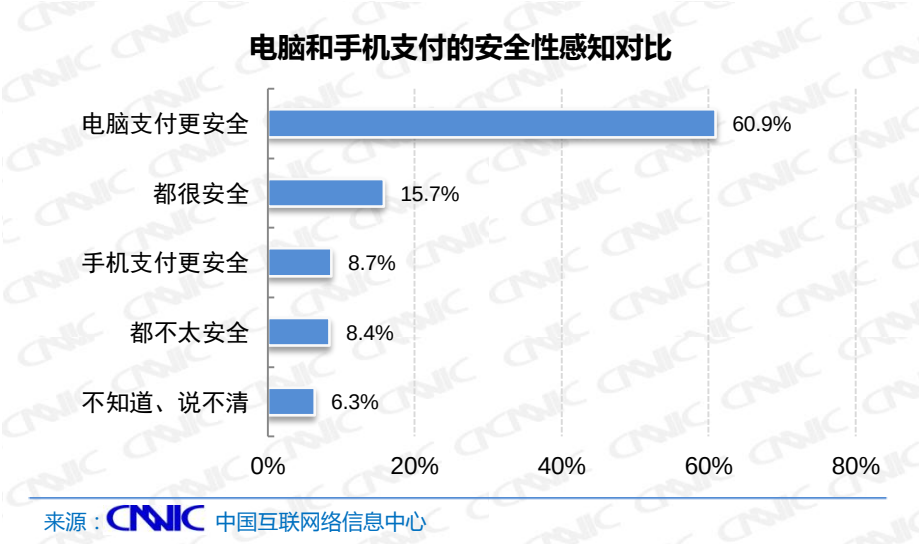


图 16 电脑和手机支付的安全性感知对比

一半以上的网上支付用户（58.6%）觉得电脑支付更安全是由于自己更熟悉电脑支付流程，熟悉度是增进安全感知的重要因素。还有 40.5%的用户是因为电脑的杀毒、防护技术更完备；34.4%的用户认为手机容易丢失、安全隐患多。还有 17.6%的用户是觉得电脑支付有

较多安全产品保障。

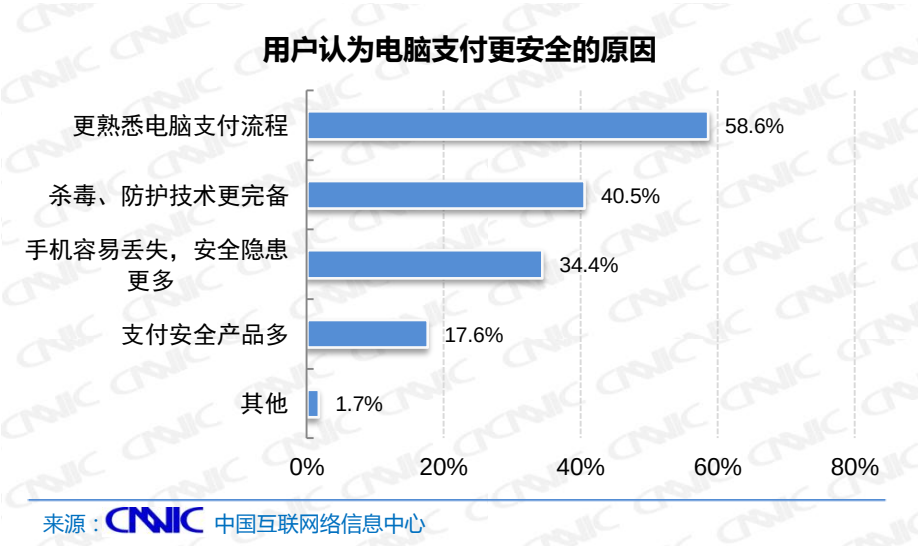


图 17 用户认为电脑支付更安全的原因

有 8.7%的网上支付用户认为手机支付更安全。最主要是因为其受恶意攻击的比例小（55.1%），其次是可随身携带（49.5%），还有 33.3%的用户是因为感觉手机支付的技术和标准更高。

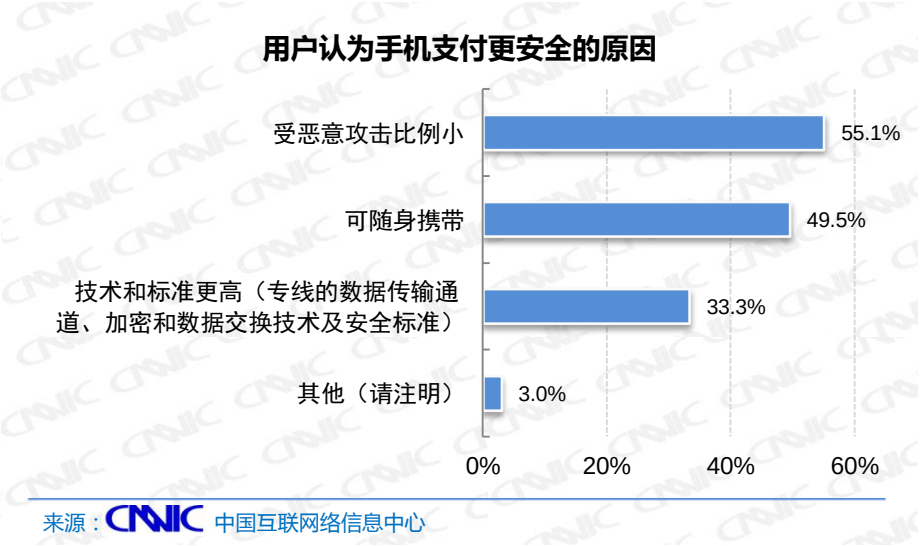


图 18 用户认为手机支付更安全的原因

网上支付用户对担保交易支付安全性评价最高

用户感觉安全性最高的支付服务类型是具有担保机制的第三方支付工具支付，如支付宝

担保交易，有 47.2%的选择比例；第二位的是普通网银支付，有 29.2%的选择比例；第三位的是具有赔付机制的第三方支付工具支付，即快捷支付，有 14%的选择比例。

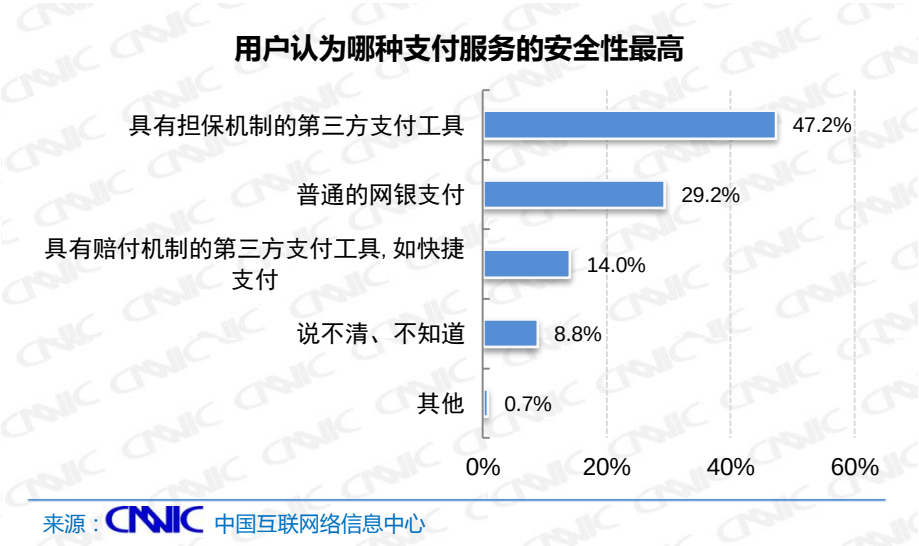


图 19 用户认为哪种支付服务的安全性最高

第三方支付中网上支付用户对支付宝安全保障评价最高

网上支付用户在对主要第三方支付工具安全保障性进行对比评价时，有 55.4%的支付用户认为支付宝的安全保障性最高，第二位的是银联在线，有 5.8%的选择比例，第三位的是财付通，有 3.5%的比例。还有 34%的用户表示说不清、不好评价。

虽然用户对比第三方支付工具的安全保障时，受使用经历和熟悉程度影响较大，但支付宝的选择比例遥遥领先，也说明支付宝的安全保证水平在用户心中具有明显的优势。银联在线拥有广泛的线下用户基础，对用户的安全信任度起到了提升作用。

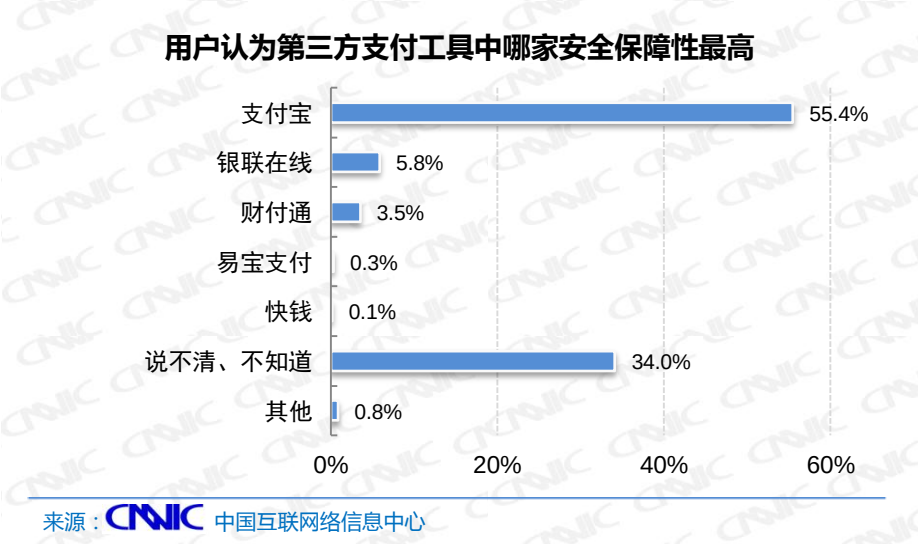


图 20 用户认为第三方支付工具中哪家安全保障性最高

网龄越长，用户网上支付安全感越强

整体来看，不同网龄的用户对网上支付的安全性评价都较高，占到 90%以上用户。深入分析发现，使用互联网的年限越长，越多用户对网上支付给予安全性的评价。网龄 1 年及以下的网民中有 6.8%的用户认为网上支付不安全，网龄在 1-2 年的网民中这一比例降为 5.4%，在网龄 5 年以下的用户中对网上支付评价为不安全的只有 3.6%。

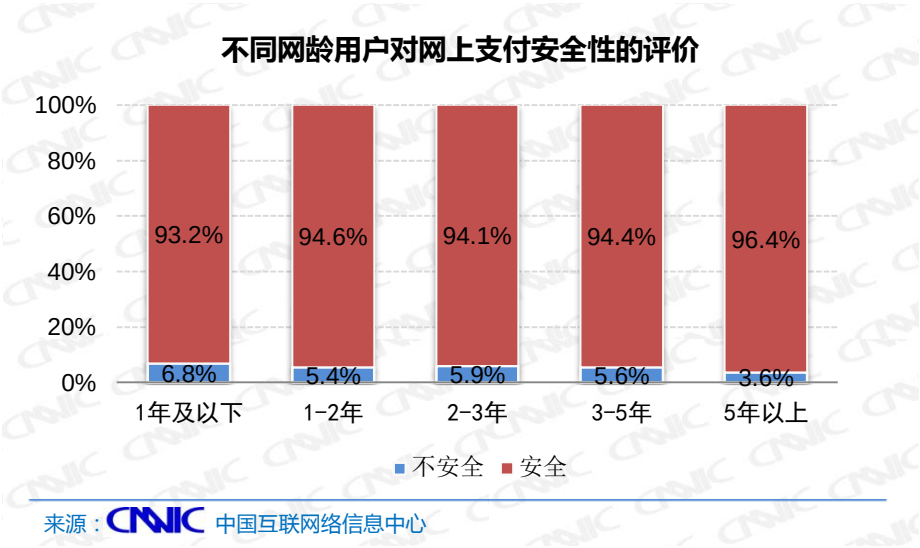


图 21 不同网龄用户对网上支付安全性的评价

4.3 用户支付安全风险防范

大部分网上支付用户使用了主要的支付风险防范措施

虽然很多网上支付用户表示对安全措施了解不多，但调查发现大部分用户实际已安装或使用了目前主流的安全措施，只有 5.6%的用户表示没有使用主要的防范支付风险的保护措施。有 71.8%的用户使用了安全厂商杀毒软件或防火墙，有 71.5%的支付用户使用了支付机构提供的安全措施（如数字证书、动态密码），还有 68.1%的用户通过设置多重密码或更高安全级别的密码来保障支付账户安全。

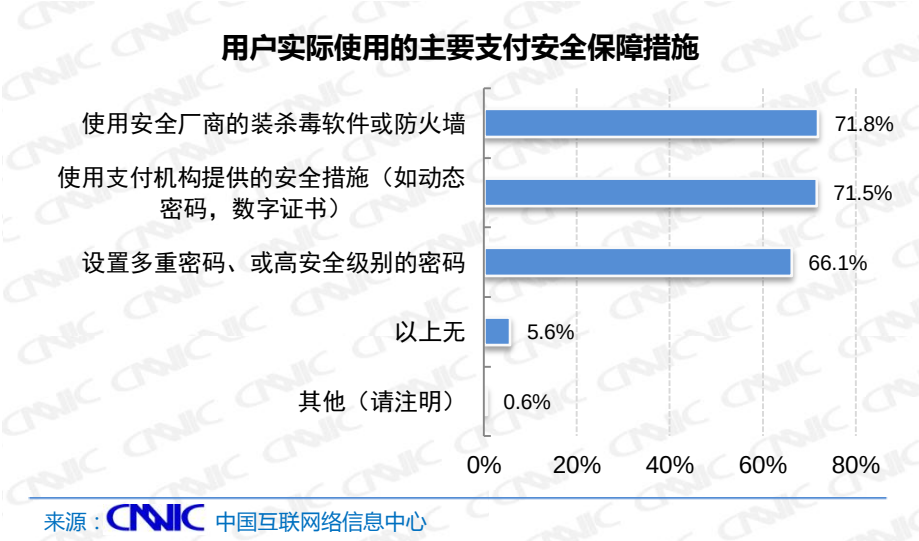


图 22 用户实际使用的主要支付安全保障措施

网上支付用户对透露个人信息警惕性高，对即时通信链接防范意识不强

网上支付用户接到电话称退款，需要告知自己的姓名、账户或手机验证码信息时，有85.3%的用户表示会拒绝透露，有 11.8%的用户会先验证对方身份，只有 2.9%的用户愿意透露信息。

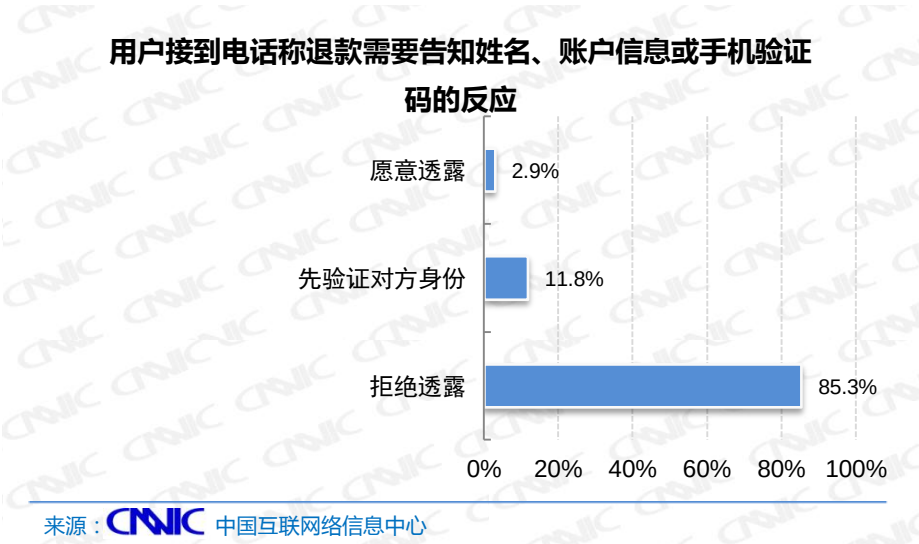


图 23 用户接到电话称退款需要告知姓名、账户信息或手机验证码的反应

用户使用即时通信工具遇到对方发来的不明链接时，有 47.8%的表示绝对不会点击，有37.2%的用户会先观察是否有安全网站标识，但有 15%的用户表示会直接点击。

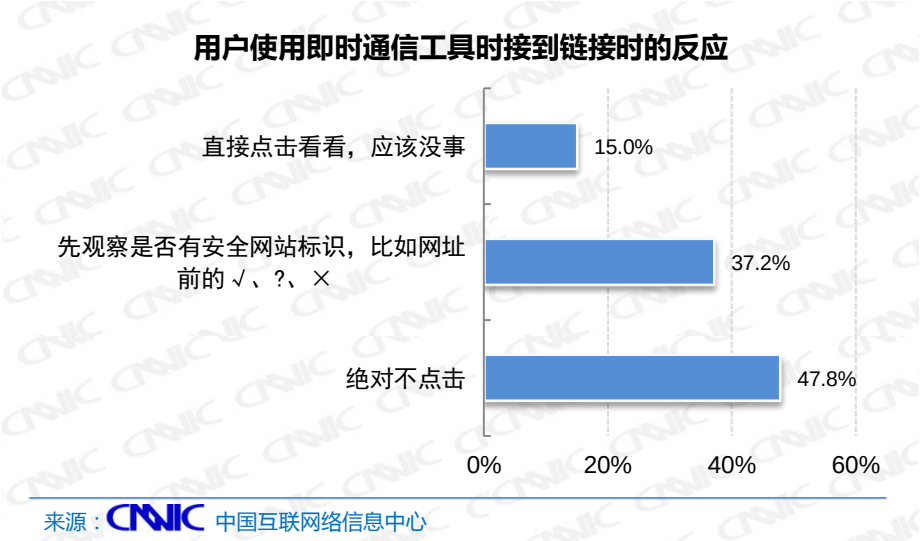


图 24 用户使用即时通信工具时接到链接时的反应

网上支付用户的不良使用习惯亦会引起网上支付的安全问题产生。首先是在使用网上支付同时下载软件、视频等，或者浏览一些新奇信息；其二是使用链接来登录支付网站，而不是通过正确的 URL 来访问支付网站；其三是对非支付网站外的风险敏感度不高，如 QQ 等即时通信发来的不明链接等，都可能造成安全风险。

4.4 安全问题处理及综合保障情况

网上支付用户遭遇支付不安全事件比例为 3.2%，钓鱼网站诱骗支付占首位

调查显示，有 3.2%的网上支付用户表示自己最近半年曾经遇到过支付不安全事件。

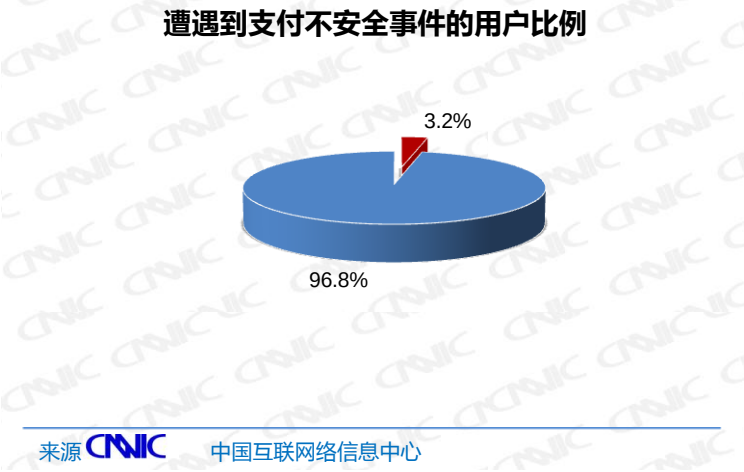


图 25 遭遇到支付不安全事件的用户比例

用户遇到的最主要不安全问题是遭遇虚假网站欺骗后贸然支付，有 64.4%的比例；第二位的是支付账号或密码被盗，有 19.2%的比例。第三位的是支付过程遭遇木马病毒、有 11%的比例。有 8.2%的用户遇到个人资料被泄漏。

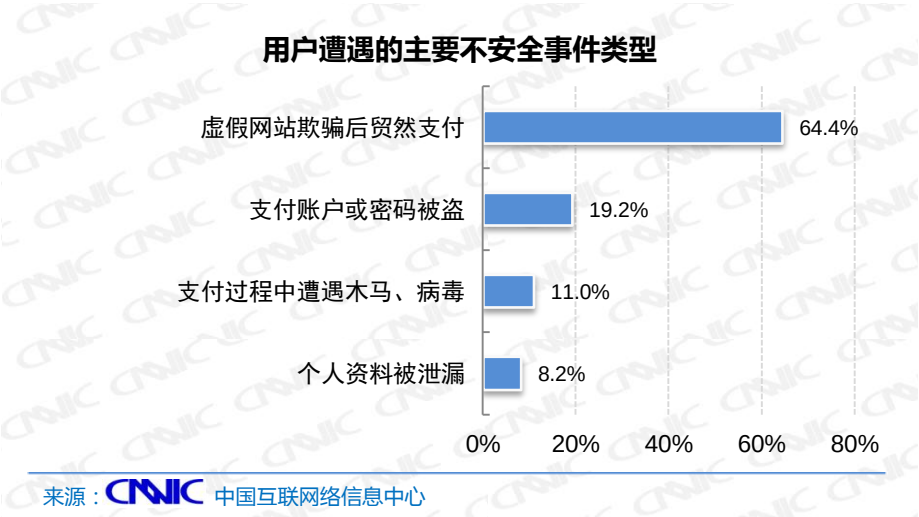


图 26 用户遭遇的主要不安全事件类型

近一半用户遭遇支付安全问题时怕麻烦没有索赔

遇到支付不安全事件的用户中，有 40%的人有实际的资金损失。在遇到不安全事件时，有 41.1%的用户并没有追究责任，而是自己承担损失。34.2%的用户是申请支付机构解决，9.6%的用户报警求助公安机关，还有 6.8%的用户自己找不法分子追偿。

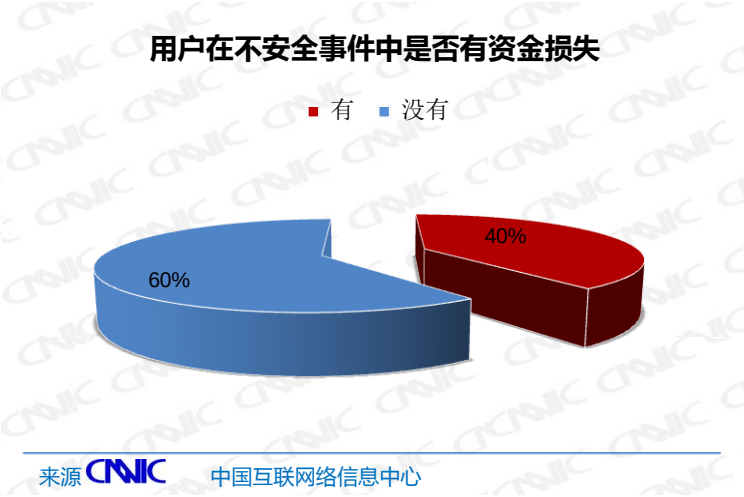


图 27 用户在不安全事件中是否有资金损失

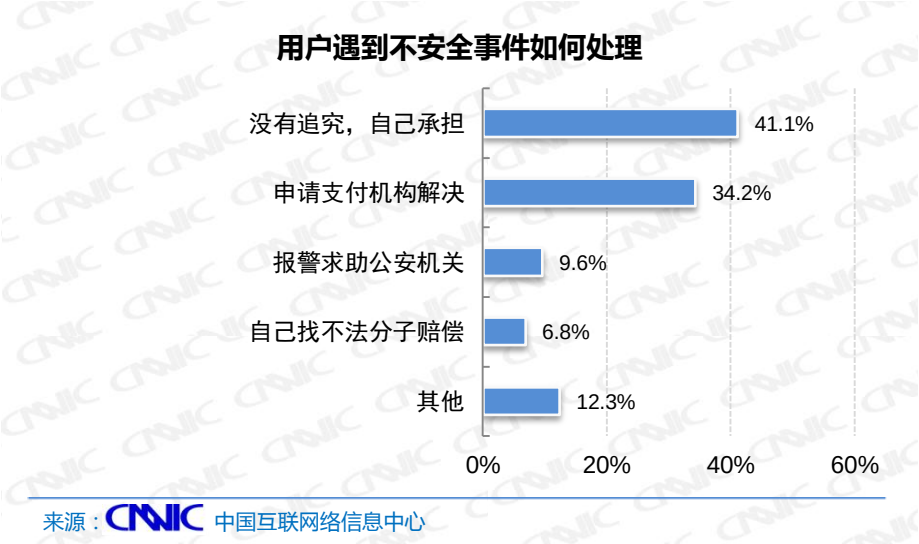


图 28 用户遇到不安全事件如何处理

56.7%的用户没有追究支付不安全问题主要是因为觉得麻烦，费时费力；还有 26.7%的用户觉得金额较小，无所谓；还有 23.3%的用户不知道怎么解决。

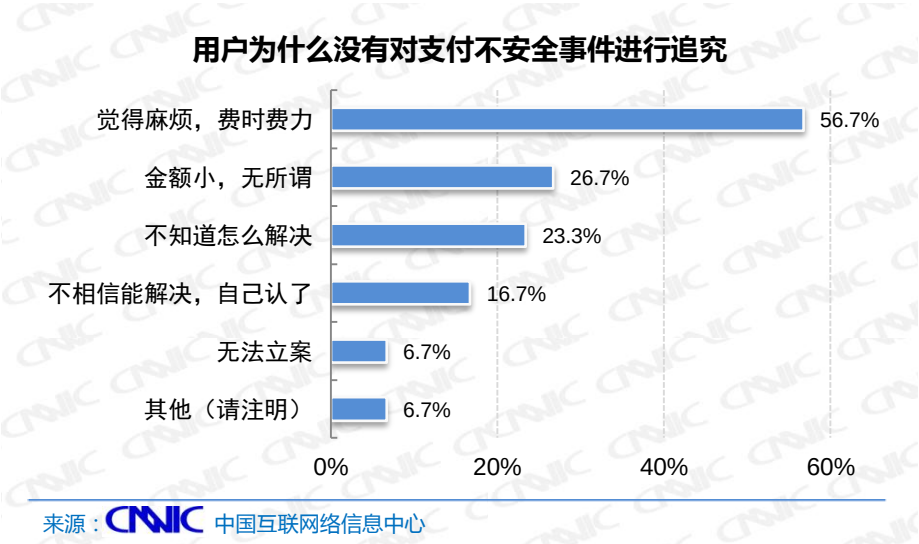


图 29 用户为什么没有对支付不安全事件进行追究

4.4 小结

从网上支付用户使用行为来看，第三方支付和网上银行支付并驾齐驱，是用户最主流的支付方式；快捷支付发展较快，已经渗透近半用户。从用户网上支付使用的安全感受来看，大部分用户都给予网上支付安全评价，比例高达 94.7%。大部分用户对电脑支付安全感知高

于手机，对担保交易支付安全性评价最高，支付安全感受设备熟悉程度和网络使用年限影响较大。

虽然很多网上支付用户表示对安全措施了解不多，但大部分用户实际已安装或使用了目前主流的安全措施。用户对透露个人信息警惕性高，但对即时通信链接防范意识不强。最近半年用户遭遇支付不安全事件比例为 3.2%，钓鱼网站诱骗支付占首位。近一半用户遭遇支付安全问题怕麻烦而没有索赔。

第五章 主要支付企业安全性对比

5.1 主要支付企业安全体系

当前主要的支付企业都较为重视安全技术，也纷纷加强了针对安全的综合保证。安全技术层面，第三方支付都采用安全套接层协议(SSL 协议)作为底层协议，客户机和服务器交换信息前都必须构建安全通道，所有信息都经过加密传输，使用页面加密技术，动态验证码登录，安全性将大为提高。此外，大部分支付平台都推荐使用数字证书，即使用户发送的信息在网上被他人截获。甚至丢失了个人的账户、密码等信息，仍可以保证用户的账户、资金安全。除了数字证书以外，支付宝还推出了手机短信的动态口令登陆的方式。财付通推出了短信验证服务、信使服务等。既可以保护用户账户安全，又为用户对数字证书的备份、导入等难题提供了解决方案。为了进一步保护用户账户安全，不少企业向金融机构看齐，不断提升安全保障措施。不少第三方支付企业提供类似于银行网银 U 盾的工具，如支付盾、财付盾，既方便了用户又保证了用户的使用安全，填补了第三方支付工具在硬件安全产品领域的空白，使得支付的安全级别达到金融业的安全级别。

综合保障方面，第三方支付平台越来越重视安全性能的开发，利用多重安全技术策略确保用户安全，大大降低了技术风。此外，以支付宝代表的第三方支付企业在赔付机制、安全教育和联盟合作方面表现突出，对用户的权益投入更多的保护，赢得了用户较多的安全信任。

但是，由于网络零售、网上预订和团购等线上交易发展速度较快，新技术、新应用不断涌现，也进入了一个问题易发期。因此网上支付企业需要在持续加强安全技术防范的同时，加强对用户保障的综合措施，从底层安全和表层体验等多方面加强支付安全建设。

表 42011 主要支付企业安全体系对比

安全组件	主要功能	支付宝	财付通	银联在线
页面加密技术	有效地保护用户资料信息			
动态校验码	防止使用穷举法进行破解			
登录安全控件	对关键数据信息进行 SSL 加密	√	√	√
数字证书	网上身份认证	支付宝数字证书且账	财付通数字证	EVSSL 数

		户必须通过实名认证机制	书	字证书服务
硬件加密技术	硬件设备提高私密性	支付盾	财付盾	——
密码保护	更加安全的保障和较高的信用度	支付宝安全客户端提供双密码保护	密码安全控件，双密码保护	
动态口令	生成不可预测的随机数字组合，提升安全性	手机动态口令，宝令安全产品	短信验证码	动态手机口令
安全监控	日常监控账户变化，支付时二次保障账户安全	“智能实时风险监控系统”，短信、邮件通知、旺旺提醒	短信、QQ、邮件通知等 24 小时安全监控系统	“风险管理系统监控 ”
赔付机制	降低用户风险，提高支付信任度	完整的会员保障机制（支付宝余额支付、快捷支付赔付机制..）	——	——
安全教育	普及安全知识，增强用户安全技巧	网站设置“安全中心”，联合各行业将热点安全问题做专题投放、互动	主页设置安全主题教育	网站“安全小常识”
联盟合作	加强安全产品的适用性，打造安全生态圈	联合全球 90%的主流浏览器和终端安全厂商，国内 TOP 商户安全合作	与腾讯系安全厂商合作更密切	与浏览器、杀毒等厂商合作

5.2 对主要支付企业整体支付安全感知对比[4]

支付宝用户对其整体安全评价最高。在主要的第三方支付企业中，用户对支付宝整体安

[4]注：本章对某一支付工具评价均是使用过该支付工具的用户做出的评价，不使用某支付工具的用户不参与对该支付工具的评价。其他第三方支付工具评价样本较少，因此仅仅对支付宝、财付通和银联在线进行分析。

全性的评价最高，有 92.1%的用户对支付宝的安全性给予肯定评价。第二位的是银联在线，评价认为整体安全的有 85.8%的用户。第三位的是财付通，安全评价比例为 83.5%。

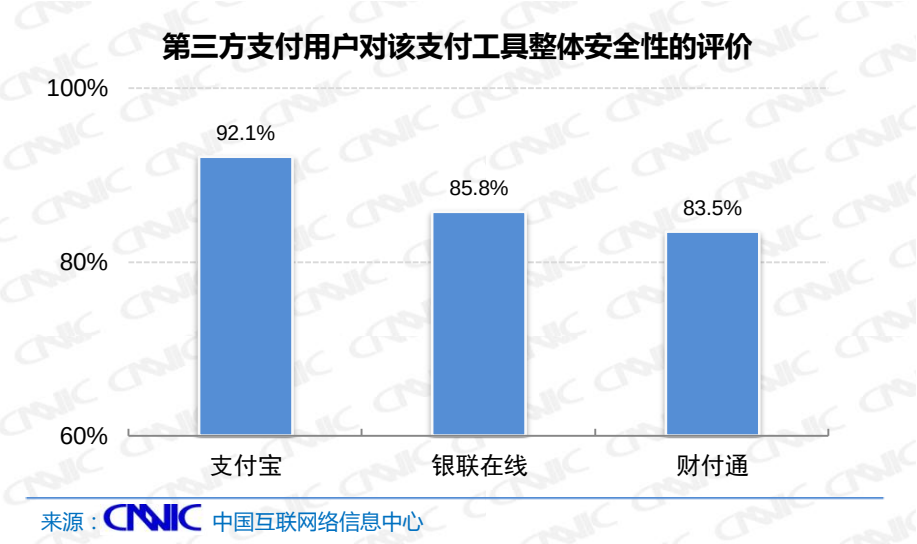
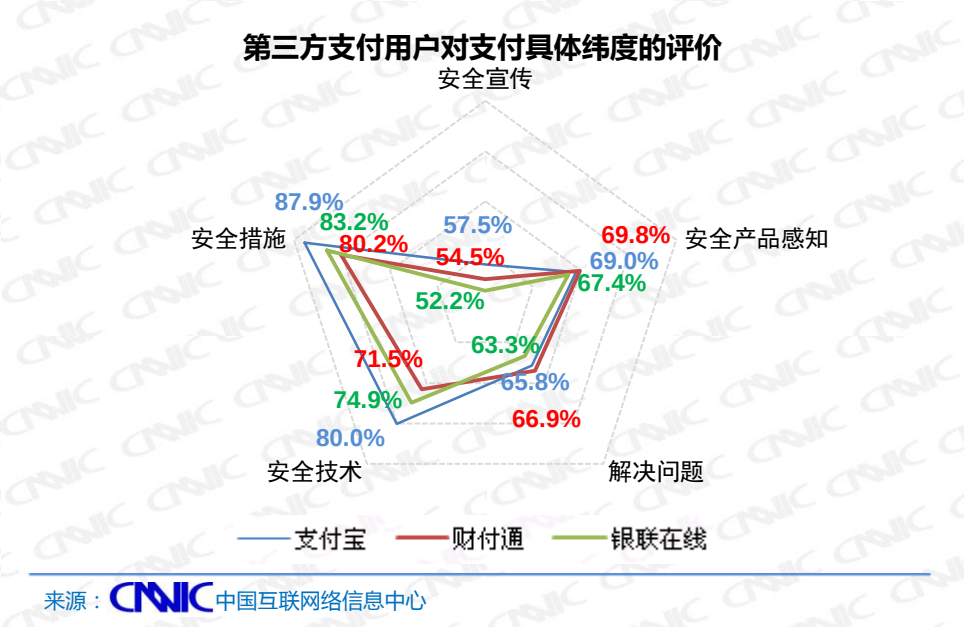


图 30 主要第三方支付工具对该支付工具整体安全性的评价

从安全技术、安全产品感知、安全措施、问题解决和安全宣传五个方面进行分别评价。可以发现，整体上看用户对主要支付企业安全技术、安全措施评价较高，有 70%-90%用户给予积极评价；用户对安全产品感知和解决问题方面的评价相对略好，积极评价占 60%-70%；用户对支付企业的安全宣传普遍评价相对偏低，积极评价用户仅占一半。对比主要支付企业，支付宝在大部分指标上的评分较为领先，但是在一些分类指标上，银联在线和财付通也表现较为突出。



	安全技术	安全措施	安全产品感知	解决问题	安全宣传
支付宝	80.0%	87.9%	69.0%	65.8%	57.5%
银联在线	74.9%	83.2%	67.4%	63.3%	52.2%
财付通	71.5%	80.2%	69.8%	66.9%	54.5%

图 31 主要第三方支付用户对支付具体纬度的评价

5.3 对主要支付企业安全技术感知对比

支付宝用户对其安全技术认可度最高。在主要的第三方支付企业中，用户对支付宝安全技术的评价最高，80%的用户认为“其安全技术处于行业领先水平”。第二位的是银联在线，有 74.9%的认同度。第三位的是财付通，为 71.5%。

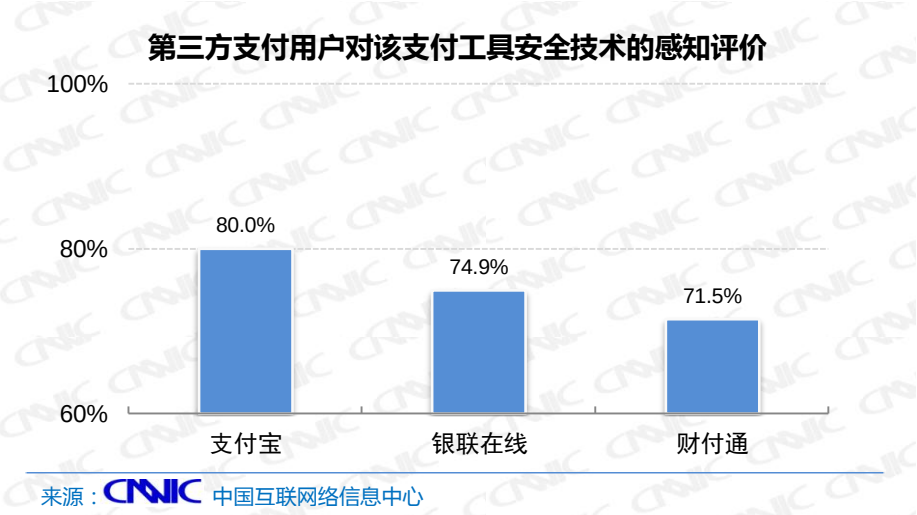


图 32 主要第三方支付用户对该支付工具安全技术的感知评价

5.4 对主要支付企业安全措施和产品感知对比

财付通用户对其安全产品认知度最高。在主要的第三方支付企业中，用户对财付通安全产品的了解程度最高，有 69.8%的财付通用户表示通过各种渠道了解其提供的支付安全产品；其次是支付宝，为 69%；银联在线比例为 67.4%。

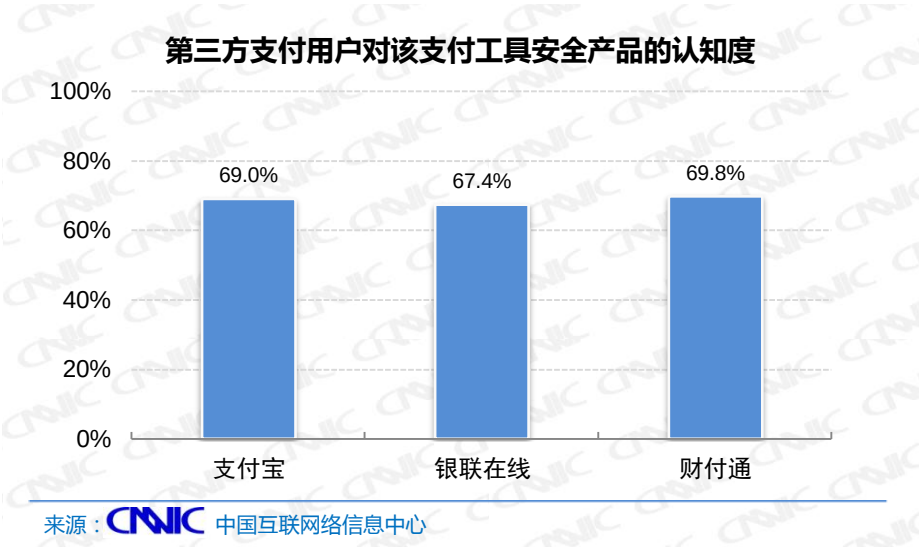


图 33 主要第三方支付用户对该支付工具安全产品的认知度

支付宝用户对其安全措施专业性评价最高。在主要的第三方支付企业中，用户对支付宝安全措施的评价最高，有 87.9%的用户认为“其采取了足够专业的安全措施来保障用户的资金安全”。第二位的是银联在线，有 83.2%的认同度。第三位的是财付通，为 80.2%。

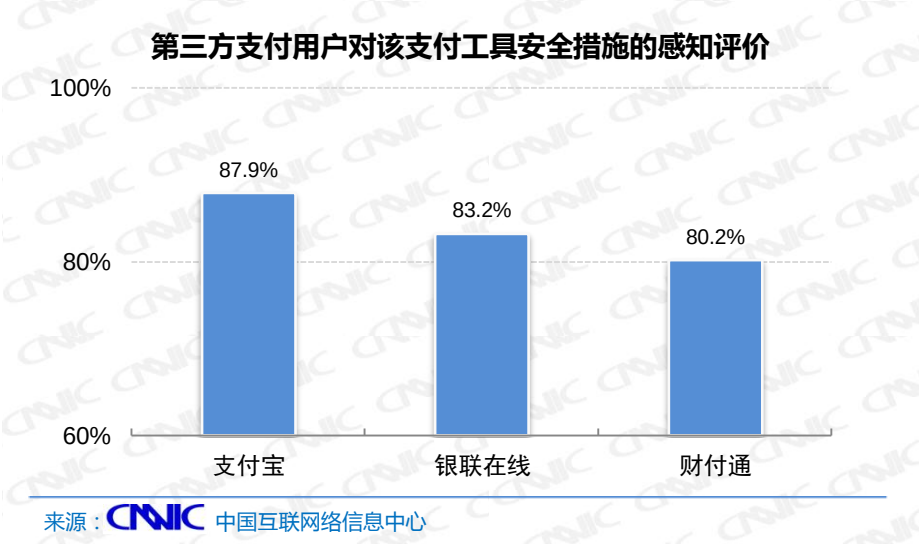


图 34 主要第三方支付用户对该支付工具安全措施的感知评价

5.5 对主要支付企业权益保障感知对比

财付通、支付宝用户对其安全问题解决能力评价最高。在主要的第三方支付企业中，用户对财付通和支付宝安全问题解决的评价较高，分别有 66.9%和 65.8%的用户对财付通和支

付宝安全问题解决较为认可，认为“一旦发生安全问题，相信其能有效解决问题”。用户对银联在线相应评价水平较低，为 63.3%。

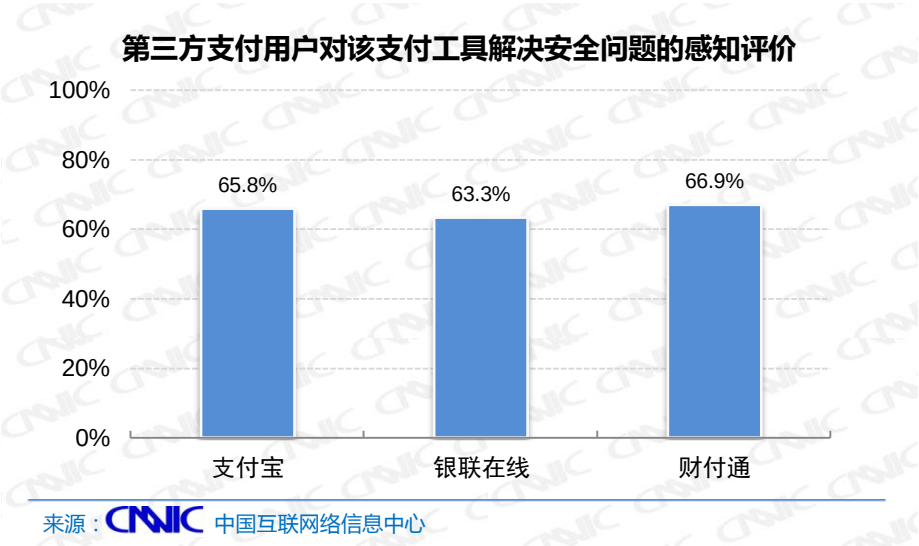


图 35 主要第三方支付用户对该支付工具解决安全问题的感知评价

网上支付用户对支付企业安全宣传感知度均不强，支付宝安全宣传在用户中普及率略优。用户对主要第三方支付企业安全宣传的认知度都不高，均低于 60%。其中用户对支付宝安全问题解决的评价相对最高，57.5%的用户表示“曾经看到支付宝做过有关支付安全知识的普及宣传”。财付通的比例为 54.5%，银联在线选择比例较低，为 52.2%。

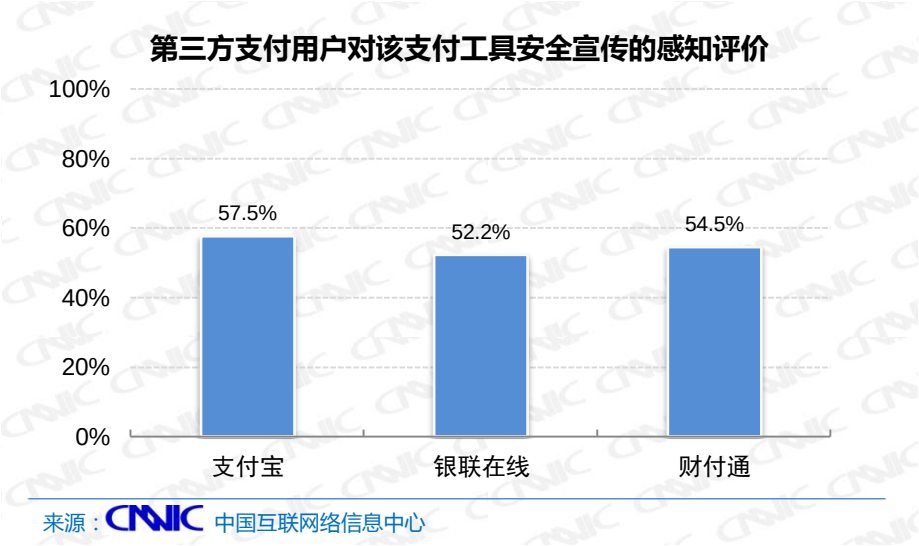


图 36 主要三方支付用户对该支付工具安全宣传的感知评价

5.6 小结

支付宝在网络支付安全体系上形成了前端短信、宝令、证书校验，后端智能风险实时监控系统，加之强有力的会员余额保障和快捷支付 72 小时赔付机制，给予用户较高的支付安全体验，明显优于其他支付企业，赢得了更多用户对其安全性的肯定。技术方面，支付宝已通过了 Verisign 签发的全球安全证书，保障客户的在线安全信息。使客户的在线交易和客户资料得到有效的保障。产品方面，通过对传统安全产品的升级，控件、宝令、证书等二次验证安全产品，实现安全产品体系保护；通过风险管控体系（智能风险实时监控系统）保护交易安全。综合保障措施方面，支付宝联合安全生态系统各环节参与者成立安全支付联盟，用户账户安全投保等，在更大程度上保证网络支付安全的同时，给用户树立支付安全信心。

银联在线发展较快，具有普遍的线下用户基础，是成长最快的在线支付机构。银联在线具有较强的安全基础，是中国首个具有金融级预授权担保交易功能的综合性支付平台，支持将交易资金在自有银行账户内冻结，无需提前向第三方划转，免除利息损失和资金挪用风险。因此在用户中有良好的信任基础，综合安全评价得分第二。银联在线也在逐步完善其安全产品，提升综合保障水平，但由于受传统业务影响，对用户在对其保护措施感受上逊于纯线上支付企业。

财付通具有较强的安全支付保障水平，借助腾讯集团内 IT 安全、QQ 等集团资源，对安全问题的处理等方面受用户好评更高，但在安全技术、安全投入和联盟合作等方面还有较大的提升空间。

第六章 网络支付安全发展建议

6.1 用户支付安全问题及防范手册

用户安全问题一：遭遇木马，盗取密码

使用户感染综合性木马，综合性木马具有屏幕查看、远程控制、键盘记录等功能。黑客利用键盘记录功能记录账号，密码、交易密码，再利用远程控制功能操纵用户计算机进行转账。

用户安全问题二：钓鱼网站，诱骗支付

不法分子冒充卖家，在用户准备交易时谎称网络有问题，发给用户一个网址链接，用户点击该链接后往往与支付页面类似。用户在该页面进行支付后，卖家说没有收到付款。当用户从通过正常登录网银查询时，也没有显示付款信息。实际是不法分子通过钓鱼网站，诱使用户支付到其他账户，导致资金损失。

用户安全问题三：冒充客服，骗取信息

不法分子冒充客服或卖家，诱使用户登录钓鱼网站，获取用户名、密码、安全保护问题及答案，然后利用安全保护问题及答案撤销手机绑定，同时避开手机动态口令限制，或者获取用户手机动态口令，盗取资金。

用户安全问题四：U 盾不拔，远程控制

用户使用完 U 盾，尤其是在公共电脑支付完后，没有及时拔出支付盾，被不法分子远程控制“借用’。

用户安全问题五：QQ 求助，贸然支付

利用用户对好友的熟悉信任度，盗取 QQ、MSN、阿里旺旺等即时通信号码后发送求助信息，要求汇款或支付资金，用户没有核实是否本人后就使用网上支付进行资金传递。或者通过 QQ 发来有危险的链接，用户由于对好友信任，贸然点击遭遇钓鱼网站或者木马病毒。

用户防范方式一：做好密码等信息保护

建议用户设置字母与数字结合的复杂密码，降低被病毒破译密码的可能性，提高计算机

系统的安全性，避免将自己的生日、姓名英文拼写、熟悉的英文单词等做为计算机系统的密码或是网上支付的密码。在聊天工具上涉及资金操作时，请一定与朋友电话确认。保护好手机校验码，不要把收到的手机校验码告诉任何人或在不明钓鱼网站输入，防止不法分子冒充支付工作人员诱骗密码。

用户防范方式二：电脑日常安全维护

经常给电脑系统升级，安装杀毒软件、防火墙，经常升级和杀毒，做好自身计算机的日常维护工作，定期给系统和相应的应用软件升级，对系统的补丁做到及时的更新，安装正式的杀毒软件和防火墙软件，并经常升级和查杀。给系统安装木马防范及系统优化软件，通过这种软件可以时时防止木马程序对自身计算机的攻击 对密码等敏感信息的窃取。尽量不要在公共电脑上使用自己的有关资金的账户和密码。支付完成后及时拔出支付盾可以避免被不法分子远程控制“借用’。

用户防范方式三：网站安全登录访问

在登录支付资金时应注意确认该网是否是官方网站，仔细核对该网的域名是否正确，注意小写 “1” 与“L” 、 “0” 与“O” 等情况；保证良好的上网习惯，访问购物网站时尽量避免手工直接输入网址方式进行访问，以免输入错误被相似钓鱼网站获取敏感信息，不点击 QQ 或即时通讯好友发来的来历不明的超级链接访问网站，以避免个人账户信息泄露或被利用，

用户防范方式四：使用安全支付产品

建议用户至少安装使用门槛较低的免费的数字证书产品，最好还能使用动态口令牌技术的安全产品，提升支付安全保障水平。

6.2 支付安全发展建议

（一）完善支付监管相关法律规章

一是基于网上支付的现状及存在的安全问题，完善相关的法律法规，与国际相关的法律接轨。继续加强对第三方支付机构的规范之路，监管重点从准入审批的硬指标管理，逐步转向风险防控和高管准入等软约束采取分级监管、提高支付机构高管准入门槛等方式。二是规范合同条款 ，保护消费者利益。需要完善社会信用机制，加快网上支付信用机制建设，使银行可以追踪客户的信用档案，确定对客户的授信额度，并将其不良行为记录纳入社会征稽体

系。三是加强对网络犯罪的监控，联合第三方支付企业、安全厂商，通过技术手段严厉打击侵犯网上支付安全的犯罪行为。

（二）加强安全支付软环境的建设

技术层面的防护是保障支付安全的硬环境，用户的自我保护和全社会的监督是保障安全支付的软环境。因此要加强网上支付安全宣传，帮助用户树立安全意识，提高消费者对网上支付平台的使用水平。第三方支付企业要更加主动利用平台帮助用户形成安全上网习惯，以及维权的意识。可以通过第三方支付工具提供的索赔程序维权的，第三方支付企业要坚决保障用户的合法权益；需要诉诸法律的，支付企业通过信息保全方式，在防止用户利益受损的同时，协助用户使用司法程序追偿损失。

（三）打造网上支付安全生态体系

支付系统安全是一个复杂的综合工程，不可能只通过单一的技术防护措施就能保证其安全性，必须施加访问控制、存储保护、身份验证、安全服务协议、入侵检测、数据备份、病毒防范等全方位的安全技术。同时，要密切关注新的网络攻击手段及其应对策略，及时更新支付系统保护技术。此外，仅仅在技术层面上的防护措施是不够的，完善的管理制度和风险防范机制、紧密配合的安全生态链尤为重要。未来需要加强由银行、第三方支付机构、安全厂商、商户、监管机构共同构筑的安全支付生态系统，甚至可以打通安全产品，为用户提供更全面的安全保护。

免责声明

本报告中的调研数据均采用样本调研方法获得，其数据结果受到样本的影响，部分数据未必能够完全反映真实市场情况。所以，本报告只提供给个人或单位作为市场参考资料，本中心不承担因使用本报告而产生的法律责任。

中国互联网络信息中心

China Internet Network Information Center（CNNIC）