

# 网络知识社区中的用户信任安全分析

胡昌平 李青青 吕美娇  
(武汉大学信息管理学院, 武汉 430072)

**摘要:** 本文通过调查网络知识社区服务中的信任传递安全状况, 分析信任传递中的安全风险因素。以此出发, 针对用户的信任偏好、认证管理滞后、恶意用户误导、不可信第三方以及服务链影响等问题, 从统一知识社区安全评价标准、完善用户身份认证制度、建立恶意用户处罚规则、加强第三方鉴定监管出发, 提出解决不安全因素影响的建议和信任安全风险管控措施, 推进用户信任安全环境治理, 为应对用户信任传递安全风险提供参考。

**关键词:** 网络知识社区; 信任管理; 安全保障

**中图分类号:** G206 **DOI:** 10.3772/j.issn.1673-2286.2021.04.005

**引文格式:** 胡昌平, 李青青, 吕美娇. 网络知识社区中的用户信任安全分析[J]. 数字图书馆论坛, 2021 (4): 31-37.

网络知识社区服务为用户分享、交流知识提供了新的交互空间, 有效地促进了知识的网络传递, 由此提出了基于信任关系的网络社区用户信息安全监管问题。事实上, 在更广范围内信任是用户决定使用服务的重要因素。然而, 网络社区用户交互中却存在误信所导致的虚假信息传播和误信任关系扩展问题。这些问题的客观存在提出了用户信任认证和安全监管的要求。知识社区中的用户信任安全保障可以应对由于误信任、采信障碍和其他不确定因素引发的信息安全风险, 确保用户无障碍地进行社区知识交互和信息安全保障目标的实现。

由相互信任引发的安全风险管控通常有两个解决路径: 一是对相关各方进行可信认证, 确保各方是值得信任的, 以消除由信任风险带来的安全隐患, 即进行可信认证和信任监管, 以保障用户信息安全; 二是按“零信任构架”进行信任安全监管与保证, 在有交互且必然存在信任风险的认知基础上, 对于各方存在程度不同的不可信, 需要进行全方位信息安全监管。实践证明, 在社会化信息安全保障中, 通过可信认证和监管保证信息安全是可行的。基于这一认识, 拟在可信云服务认证基础上, 进行针对网络知识社区的信任安全保障拓展。

## 1 基于信任传递的网络知识社区用户信任安全调查

在网络知识社区服务及其安全保障中, 一方面, 社会关系、声誉、基于第三方的信任、加入某类组织等都能说明个体具有可信度, 完全陌生的个体也可以据此建立信任关系; 另一方面, 基于信任响应的信任关系也是由于一方先信任另一方而建立起来的, 陌生的个体间完全可能由于一方对另一方先采取信任策略而最终建立信任关系。然而, 这种信任建立过程中的不安全因素必然带来信任危机。因此, 有必要针对网络知识社区信任安全进行系统性分析。

### 1.1 基于信任传递的调查模型

当前对网络知识社区信任问题的研究主要集中在两个方面, 即社区中信任建立的影响因素以及信任在知识社区中的作用机制。知识社区中信任关系的建立主要受3个方面因素影响: ①个体因素, 如性别、年龄、教育背景、个人信任倾向等; ②成员交互因素, 包括人人交互和人机交互; ③系统因素, 如系统易用性、稳定性、可靠性等都会影响社区成员对系统的信任建立<sup>[1]</sup>。从安全角度来看, 信任关系是影响用户使用知识社区的关

键性因素,可直接作用于用户使用意愿,也可通过影响其他因素而对使用意愿产生间接的作用<sup>[2]</sup>。诸多学者通过实证研究表明,当与人之间的社会关系处于高度信任时,一般会更愿意参与社会交往和知识交流<sup>[3]</sup>。同时,人际信任对用户的知识交流存在正向显著作用,个体的行为、主体认知和环境交互影响具有普遍性,即交互信任可直接影响用户的使用行为,也可通过主体认知对用户行为产生间接作用。其中,主体认知包括对自身行为的感知和对虚拟知识社区的感知<sup>[4]</sup>。

信任问题作为知识社区管理的难点和关键,虽然引起广大学者的关注,但目前的研究大多集中于定性分析信任影响因素和信任对提高用户使用意愿的作用方面,对信任带来的安全问题研究有所欠缺。为解决网络知识社区信任传递中的不安全问题,本文拟从网络知识社区信任传递链出发,以网络知识社区用户为调查对象,采用问卷调查方式,从人际信任传递和制度信任传递出发,调查用户使用网络知识社区时由于信任传递而引发的安全风险,在此基础上对突出的安全因素进行影响因素分析,进而提出相应的安全保障建议。

按Wu等<sup>[5]</sup>的理论可将网络知识社区的信任归纳为人际信任和制度信任。其中,网络知识社区中的人际信任主要指信任关系在社会网络中的传递,包括用户实质性人际交往、相关知名社区用户信任和社区用户的评价信任;制度信任主要指网络知识社区用户对于知识社区服务和知识社区平台的信任。

基于人际信任的传递形式主要包括在现实的交往中由于对网络知识社区某用户的认知和能力有很高的期望,通过对该用户的信任而间接信任知识社区。其中,该用户对知识社区的信任起源也可以是多方面的,如声誉极高的用户入驻某一网络知识社区,其他用户可能出于对该用户的声誉了解而选择相应的知识社区;另外,用户也可能因为参考了知识社区的其他用户评价而信任知识社区。

基于制度信任的传递形式包括:由于相信知识社区服务进而信任其组织下的知识社区;由于信任知识社区的合作方进而信任知识社区;由于信任知识社区的身份认证机制,进而信任经由其认证的领域专家;由于信任第三方鉴定机构对网络知识社区的认证,进而信任知识社区。从用户到知识社区之间的信任关系上看,可进行人际信任和制度信任的多种组合。

从网络知识社区信任传递关系出发,在基于信任关系的安全保障研究中,确立本文的问卷设计思路。在

问卷调查中,将问卷分为两大部分,分别是调研对象背景和使用知识社区中由于信任引发的不安全问题。首先,可以了解受调查人员是否使用和熟悉网络知识社区以及通过信任传递方式接纳网络知识社区服务过程,以反映一系列基本情况,提问项包括学历层次、专业、使用的网络知识社区、使用知识社区的年限以及使用频率;其次,通过何种信任传递方式接纳网络知识社区,以及使用知识社区服务后的信任评价等进行信任安全分析。按Abdul-Rahman等<sup>[6]</sup>提出的定性的信任模型,将信任分为非常值得信任、值得信任、不值得信任和非常不值得信任4个层次;以此出发,在用户信任传递中进行信任的等级评价。

## 1.2 网络知识社区用户信任安全调研

根据网络知识社区信任传递链,可进一步明确网络知识社区用户在信任传递过程中遇到的具体问题。因此,本文调研了小木虫、丁香园、知乎、科学网等网络知识社区平台的帮助文档、用户评论、社区论坛、政策文档等,同时辅助以信任安全、信任管理等主题的文献,制定个人访谈和焦点会议大纲。访谈对象包括部分高校的42名博士研究生、教师及科研人员。通过调查和分析,将所存在的知识社区信任传递过程中的不安全问题归纳为两个方面的7个关键问题(见表1)。根据问题是否发生过和对用户造成的影响,设置“发生过且影响很大”“发生过但影响一般”“发生过但没太大影响”“没有发生过”4个选项。

表1 网络知识社区服务信任传递过程中的不安全问题

| 信任分类 | 不安全问题                 |
|------|-----------------------|
| 人际信任 | 信任偏好等个体因素引发的信任安全风险    |
|      | 名人效应引发的信任安全风险         |
|      | 参考知识社区中的用户评价引发的信任安全风险 |
| 制度信任 | 知识社区运营商的品牌效应引发的信任安全风险 |
|      | 知识社区服务链信任引发的信任安全风险    |
|      | 知识社区的身份认证制度引发的信任安全风险  |
|      | 鉴定制度不健全引发的信任安全风险      |

在正式发放问卷前,通过进一步的用户访谈和焦点会议修正了问卷提问,以解决专业术语理解困难、问项表述模糊等问题,最后进行规模性问卷设计。由于高校硕、博士研究生及教师为网络知识社区的重要服务对象,因此针对高校硕、博士研究生和教师发放纸质问

卷和网络问卷具有代表性,接受网络问卷调查的对象包括全国各地的数十所高校研究生、教师和科研人员。问卷发放、回收时间为2020年8月,历时15天。

本次调查共收回问卷411份,有效问卷378份,有效回收率为92.0%。73.2%的受调查人员使用两种或者两种以上的网络知识社区,88.3%的用户使用知识社区超过一年,且65.4%的用户使用网络知识社区的频率为一周3次以上。87.1%的用户都使用过知乎。另外,用户使用比较多的知识社区有豆瓣、丁香园、小木虫、科学网、天涯、果壳、经管论坛等。

为保证调查数据的准确性,通过统计软件SPSS 20.0对调查结果进行信度检验。对问卷的统计数据分别进行信度检验,Cronbach's  $\alpha$ 值分别为0.816和0.793。Cronbach's  $\alpha$ 系数大于0.700,认为问卷之间的一致性较好。由于本文的调研目的是为了确定信任安全障碍,故主要进行内容效度验证。本文采用专家逻辑分析法,通过信息安全领域的专家对调查提问与期望测定内容的符合性判断,采用内容效度比计算方法计算问卷条目水平,量表除条目5(恶意提供虚假的使用体验,诱导用户接受知识社区服务)的内容效度比CVR(Content Validity Ratio)为0.67以外,其他条目内容效度指数均在0.97以上;量表水平的内容效度指数S-CVI(Scale-level CVI)采用S-CVI/UA计算方法,两个量表的S-CVI/UA分别为1.00、0.90,内容效度较好。

## 2 网络知识社区用户信任安全影响因素与安全风险分析

调研结果显示,28%的用户通过信任传递方式使用网络知识社区服务后给出的信任评价为不值得信任,9%的用户认为被推荐的知识社区非常不值得信任。进一步分析表明,网络知识社区信任传递过程中的安全问题主要集中在不同实体的信任偏好不同、利益驱使、恶意引诱以及鉴定制度不健全等方面。

### 2.1 个体因素引发的信任安全风险

当用户具有使用知识社区的需求时,周围熟悉人的使用体验会成为最易获取的参考,而且他们对社区知识内容、安全性能、服务质量的感知会在很大程度上影响其他用户的使用意向,他们对知识社区的信任会更容易传递给社区关联用户。然而,也有大量的用户因现实

活动中熟悉人的推荐,而选择使用了网络知识社区,结果和预期中的使用体验有很大落差,体现为因错误选择对用户造成不安全影响。引发这一现象的具体原因如表2所示,首先是推荐用户和被推荐用户的安全需求不同,推荐用户可能不太关心信息的完整性或者隐私安全等,而这对被推荐用户来说却显得非常重要;其次是双方的知识背景不一致导致的推荐风险,如推荐者具备某专业网络知识社区所涉及的知识领域背景,而被推荐用户则不曾涉猎该知识领域,以至于该专业知识社区对于用户来说过于专业化,理解不了。这说明双方的教育背景和理解能力存在较大的差异,如推荐者的水平较高,把自认为很好的知识社区推荐给了熟悉的人,而被推荐者不具备相应的能力,那么会导致被推荐用户的安全使用体验很差。

表2 个体因素引发的信任安全问题类型及其影响占比 %

| 问题类型      | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|-----------|----------|----------|-----------|-------|
| 安全需求不同    | 7.2      | 15.3     | 34.4      | 43.1  |
| 知识背景不同    | 3.4      | 7.4      | 26.7      | 62.5  |
| 学习、理解能力不同 | 1.6      | 2.1      | 10.3      | 86.0  |

### 2.2 用户评价和名人效应引发的信任安全风险

当用户对知识社区或者知识社区的某些内容不熟悉时,参考社区中的用户评论往往是最便捷的方式。但是,被调查用户也有可能因参考用户评价而选择与预期不符的知识社区服务。造成这一现象的原因如表3所示,首先,一些用户出于某种利益或者和内容发布者的特殊关系,故意美化或者推荐知识社区不存在的优点,将一些不正确或者没那么权威的内容描述成真实、可信的知识,引诱其他用户采纳错误的知识信息或者不完美的知识社区服务;其次,一些用户出于某种报复心理,故意隐瞒自己的不好体验,夸大或虚构知识社区中某种服务或知识内容,诱导更多的用户重蹈他们的覆辙;最后,内容发布者会采取一些技术手段控制评论,将负面的评论予以屏蔽。

大量用户熟悉的名人或者权威人士入驻网络知识社区会极大地吸引用户的追随。然而经调查发现,有的用户因为大量专业领域内权威专家的入驻,而选择使用网络知识社区,结果使用体验并不如意。调查结果如表3所示。造成这一问题的首要原因是网络知识社区通过利益

引诱知名人士入驻,而知名人士在知识社区内并未有太多的知识共享行为,只是一种挂名行为;另一原因是知识社区的知名用户或者认证专家接受了品牌方的某种请求而传播虚假信息,从而引发用户的不信任甚至反感<sup>[7]</sup>。此外,一些权威专家出于某种心理会夸大自己的知识领域影响力,发表一些自己不太擅长的领域言论,而误导用户。由于知识社区的自由度较高,在缺乏进一步监管的情况下,必然存在不实言论所引发的安全风险。

**表3 用户评价和名人效应引发的信任安全问题类型及其影响占比** %

| 问题类型   | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|--------|----------|----------|-----------|-------|
| 利益驱使   | 2.9      | 6.1      | 16.4      | 74.6  |
| 恶意诱导   | 1.8      | 2.4      | 9.8       | 86.0  |
| 控制评论   | 0.8      | 2.9      | 10.9      | 85.4  |
| “僵尸”名人 | 3.2      | 7.1      | 17.8      | 71.9  |
| 宣传性诱导  | 6.1      | 12.4     | 27.0      | 54.5  |
| 非专业性言论 | 1.9      | 2.4      | 3.4       | 92.3  |

## 2.3 鉴定制度不健全引发的信任安全风险

网络信任评价机构作为第三方,应具有较高的可信度,领域专业机构或行业协会通过一系列标准和严格的认证程序来保证通过认证的领域知识社区服务是值得信任的,最终提供的标识作为一种认证标签而存在。用户对权威鉴定机构的信任可以传递给通过这些机构认证的网络知识社区,所以他们对网络知识社区的评价会在很大程度上影响用户对网络知识社区的信任。但是,依然有用户在选择拥有第三方鉴定资质的网络知识社区认证后,体验不到应达到的服务品质。造成这一问题的主要原因如表4所示。第一,网络知识社区为了提高信誉和彰显服务水平,会通过某种利益形式,使得第三方鉴定机构违规操作,以授予不合格网络知识社区合格资质;第二,对于一些新兴网络知识社区,第三方鉴定机构可能存在鉴定标准体系不完善、鉴定程序不完整等问题;第三,有一些鉴定机构,可能在不具备鉴定资质的情况下,违规授予网络知识社区一些不被权威机构认可的资质证书。对此,在信息安全认证中应进行严格的合规监管。

## 2.4 品牌效应引发的信任安全风险

用户比较容易信任知名度高、品牌形象好的网络

**表4 鉴定制度不健全引发的信任安全问题类型及其影响占比** %

| 问题类型    | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|---------|----------|----------|-----------|-------|
| 鉴定程序不合规 | 1.1      | 2.9      | 4.5       | 91.5  |
| 鉴定标准不完善 | 1.9      | 5.0      | 7.1       | 86.0  |
| 鉴定资质不健全 | 2.4      | 3.4      | 6.6       | 87.6  |

知识社区。一方面,因为网络知识社区的品牌知名度建立不容易,如果违背了用户的信任意愿他们所遭受的损失显而易见,所以一般不会轻易违背用户的信任。另一方面,知名度和品牌在很大程度上来自于信任传递影响力的发挥、宣传以及知识社区的用户口碑。通常情况下,用户对于公共媒介机构的信任度是比较高的,所以用户会将权威媒介机构的信任转移到其所报道的网络知识社区服务上。调查显示,有部分用户是因为网络知识社区的名气而选择其服务,如果发现品质和名气不符,必然产生负面影响。造成这一问题的原因如表5所示,一是权威媒体出于利益关系,对网络知识社区进行大力度宣传,而对其服务品质并不太了解,或者是故意隐瞒其缺点、放大其优点。二是拥有大量用户和好口碑的网络知识社区,也可能是知识社区通过某种利益关系诱导用户的结果,如赋予用户可以享受某种权限等,好口碑的形成也可以通过奖励给予好评的用户额外的服务来实现。所以网络知识社区的高名气形成过程,也可能存在相应的信任安全风险。

**表5 品牌效应引发的信任安全问题类型及其影响占比** %

| 问题类型     | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|----------|----------|----------|-----------|-------|
| 虚假宣传     | 2.1      | 4.0      | 6.9       | 87.0  |
| 名不符实的用户量 | 1.6      | 7.7      | 13.5      | 77.2  |

## 2.5 认证制度不健全引发的信任安全风险

很多用户在入驻网络知识社区时,尤其是对于分享知识的信息用户,知识社区会对他们的身份进行认证,以使他们的言论更具可信性,对于其他用户,也更容易采信已认证用户提供的知识信息。调查显示,有相当部分的用户,正是受认证用户的影响,误信了不严谨甚至虚假的信息。因为这些已认证的用户中可能存在某些伪专家,他们利用网络知识社区身份认证制度的漏洞,提供虚假的身份认证信息或发布一些内容质量不高甚至不正确的信息,从而误导其他用户下载甚至购买不实产

品。造成这一问题的原因如表6所示, 主要是网络知识社区对认证用户的监管不严格, 如有些知识社区对学历进行认证只需要用户提供学校、专业等表层信息, 对职业的认证也存在一定的缺陷。另外, 用户的注册信息存储和保密机制不健全, 很容易被恶意用户窃取, 存在冒用认证用户的身份, 以认证用户的名义发布误导信息的风险。此外, 恶意用户的注册信息和知名用户的注册信息难以判别, 从而引起用户的误认。

表6 认证制度不健全引发的信任安全问题类型及其影响占比/%

| 问题类型       | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|------------|----------|----------|-----------|-------|
| 用户身份造假     | 2.9      | 4.0      | 4.5       | 88.6  |
| 认证用户账号被冒用  | 1.3      | 3.2      | 5.6       | 89.9  |
| 知名用户身份鉴别有误 | 4.5      | 6.1      | 26.7      | 62.7  |

2.6 网络知识社区服务链信任传递引发的信任安全风险

互联网技术的快速发展使网络信息服务的分工越来越细, 很多网络知识社区越来越关注自身的领域扩展, 而把整个服务流程中的一些非核心部分通过与合作伙伴联盟来完成。如有些网络知识社区并没有自己的硬件设备, 而是通过云服务等方式外包给第三方; 还有一些网络知识社区没有自己的知识资源, 而是通过和专业的知识信息资源服务商合作来提供相应的服务<sup>[8]</sup>。对于用户来说, 一些合成性的服务安全保障大多基于合作信任关系来实现, 这说明, 对于合作伙伴的信任将直接影响对于该网络知识社区的信任, 所以选择可信的合作伙伴对于知识社区信任安全具有关键性作用。如表7所示, 部分用户因为信任网络知识社区的合作伙伴而选择了该知识社区, 因此知识社区的服务和合作伙伴的服务安全品质的匹配具有重要性。造成这一问题的原因有某些知名的知识内容服务提供商为了扩大自己的业务范围和便捷地把知识传递给用户, 往往会增加知识服务社区功能板块, 但由于其非核心业务投入有限, 知识社区的服务合作必然面临信任风险规避问题。此外, 知名合作方也会由于审核不严格, 而和一些低品质网络知识社区进行合作。另外, 网络知识社区也会由于对云计算服务商等合作伙伴了解不全面, 而选择不合格的合作伙伴。

从调查中发现, 以上多方面安全风险的存在具有客观性, 虽然大多数用户没有受到其全面影响, 然而所

表7 服务链信任传递引发的信任安全问题类型及其影响占比/%

| 问题类型              | 发生过且影响很大 | 发生过但影响一般 | 发生过但没太大影响 | 没有发生过 |
|-------------------|----------|----------|-----------|-------|
| 合作商可信, 知识社区不可信    | 0.8      | 1.9      | 3.4       | 93.9  |
| 知识社区平台可信, 知识社区不可信 | 1.3      | 2.4      | 2.9       | 93.4  |
| 知识社区可信, 服务商不可信    | 2.1      | 3.7      | 6.9       | 87.3  |

存在的安全威胁必须面对。

3 网络知识社区用户信任安全监管的完善

通过对网络知识社区用户信任传递中的安全问题的分析, 发现引发信任传递的安全因素是多方面的。其中, 不同实体的信任偏好差异、利益驱使下的非规行为、制度不完善和恶意传递等问题最为突出, 因此需要从基本的安全问题出发, 完善网络知识社区服务中的信任传递规则, 为实现网络知识社区的安全利用提供保障。

3.1 统一网络知识社区信任评价标准

不同的网络知识社区用户需求、使用目的和网络平台性能要求各不相同。因而需要制定一个普适性的网络知识社区用户信息安全需求表达规范, 以引导用户充分表达自己的要求, 为网络知识社区信任传递和安全保障提供支持。从现实问题上看, 知识社区信任安全评价规范应包括用户所需要的网络知识社区类型, 使用网络知识社区服务的安全目标, 所需要的领域知识信息以及对所需知识领域的认知信任水平和用户学习能力。此外, 对网络知识社区服务中的知识产权要求、隐私安全要求、知识社区平台的信任稳定性评价等也需要确认。网络知识社区中知识内容的准确性、完整性和安全质量方面的要求也应具有针对性。

某一用户接受熟悉的网络知识社区其他用户推荐之前, 也需要了解对方的评价标准。其中, 每一个用户对同一个网络知识社区的评价, 因评价标准和评价指标不同, 也会给出不同的结果<sup>[9]</sup>。针对网络知识社区规范的评价指标体系构建可以有效解决这一问题。其评价体系对应于网络知识社区的需求, 评价内容包括网络知识社区的类型、知识信息的专业化程度、知识产权、

用户隐私、知识信息安全质量、知识社区平台安全信任等。此外,向身边的人推荐网络知识社区的前提是推荐者对该知识社区有充分的了解,因此也需要对用户信任传递进行评价和管理。

### 3.2 建立知识社区恶意用户惩处机制

网络知识社区中存在的虚假信息 and 评论往往由匿名用户引发,随意传递不可信评论的行为发生,是由于网络知识社区无法对匿名者进行追责,也不会对他们的现实声誉带来实时影响<sup>[10]</sup>。针对网络知识社区中的恶意用户或者发布不实评论的用户,可以采取实名指证的方式,从而使这些违规行为变得可以追责到现实中的具体用户,从而增加用户的信誉危机。例如,赋予实名认证的用户更多的权限或者对实名评论的用户给予奖励等;也可以给用户设置信誉值作为他们在知识社区内权限的评判依据。实名评论可以得到更高的信誉值,而故意提供不实评论则会被扣除一定的信誉值<sup>[11]</sup>。

针对网络知识社区中专家行为导致的信任传递失效问题,可以对每一个专家认证用户设置一个考核等级,而考核的标准应该包括该用户在知识社区内的实质性知识贡献度。一般而言,用户发布的知识信息越准确、向其他用户安全传递的知识越多,知识贡献度就越高,获得的认证等级也就越高。对于安全传递信息的等级评价,可以防止某些认证专家的不实挂名<sup>[12]</sup>;同时,应对网络知识社区中专家共享的知识信息进行过滤,对于涉及的宣传性知识内容进行可信性审核。对于认证用户和宣传内容方的利益关系,应予以实时判别。另外,应为每个权威认证用户标明所擅长的知识领域,以供其他用户确认其共享知识的安全可信性。

### 3.3 加强网络知识社区的监管力度

由第三方检测机构引发的网络知识社区中的信任传递不安全问题,建议从以下方面进行改进。第一,对已经授予检测资质的第三方机构,加强对实际检测中的监管以及工作结束后的事后监管,如设立第三方检验机构行政许可制度,规范对他们的管理,防止违规操作的发生。第二,在实施中,应完善第三方鉴定结果采信管理,并开展安全责任追溯。对于新兴的网络知识社区,应动态调整信任安全检测指标,改革检验鉴定模式,进行有效的监管介入和差异化实施。第三,针对第

三方机构由于缺乏行业约束机制的情况,加强追责管理。只有符合有关法律、行政法规、规章制度要求和技术能力、人员资质条件的机构,经有关部门审核批准,才能获得许可,以规范网络知识社区安全鉴定服务。

由品牌效应引发的网络知识社区传递的虚假广告和对网络知识社区的夸大失实宣传,或者宣传语义模糊,必然使用户误解,从而使用户对知识社区的真实情况产生错误的联想,其安全信任监管必须强化。另外,网络知识社区由用户量和用户好评形成的品牌形象,理应进行评测。针对以上问题,建议作出以下改进:加强整治夸大夸张宣传、误导用户等知识社区的品牌形象传播;依法追究虚假广告行为的行政责任和民事责任,严重者需要追究其相应的刑事责任。对于网络知识社区有意控制用户评论、屏蔽负面评论的行为,应该规范平台的删帖、屏蔽等控评行为。对于网络知识社区中的违法、谣言等信息,应实时监控。与此同时,对于用户发表的合法评论,网络知识社区平台应充分尊重和进行安全维护。针对网络知识社区平台采取某种手段,如通过权限设置来圈定大量含水分的用户行为,会致使社区降低用户的好感度,因此应给予用户一定的体验权限,以通过良好的使用体验吸引用户获取更高的满意度。

### 3.4 完善知识社区用户和服务的可信认证

针对网络知识社区中的认证安全问题,建议从以下方面着手改善:首先,严格审核容易误导用户的恶意注册信息,实名认证过程中需要用户提供身份凭证;其次,针对所有的认证凭据,在对应的信息库中核实真伪,以提高网络知识社区用户信息真实性和安全性;最后,维护用户的隐私权和名誉权,同时在知识社区中对用户信任等级进行标识,用以区分相似用户。在知识社区服务中,可按用户的信任传递关系进行用户发布信息的可信性评价,并按可信认证标准进行规范管理。

针对网络知识社区服务链引发的信任传递失效问题,建议从以下方面改善。首先,建立完善的法制化保障体系,网络知识社区服务链上的主体一旦出现信任危机,将损害他方利益或导致安全事故的发生,因而应受到相应的惩罚。其次,对于网络知识社区间的信任关系维护,应建立在规范化的信任评定基础之上,这就要求专门机构承担资信评定工作。在评定中,要以独立、客观和公正为原则进行认证和监管。最后,应在网络知识

社区信任认证中制定统一的规则 and 标准, 从而保障知识社区主体信息安全和用户信任传递安全, 最终保障用户信息安全和知识社区交互安全。

## 4 结语

本文通过对网络知识社区的信任传递及安全问题调研, 发现信任偏好、恶意用户引诱、第三方鉴定监管缺乏、用户身份认证不健全、服务链不可信是引发网络知识社区服务中的信任传递安全的主要障碍, 因而应通过统一网络知识社区信任评价标准、构建恶意用户惩处机制、加强网络知识社区鉴定监管、完善网络知识社区用户和服务方认证体系, 进行网络知识的安全治理, 以实现知识社区交互信息安全保障目标。

## 参考文献

- [1] 陈小卉, 胡平, 周奕岑. 知乎问答社区回答者知识贡献行为受同伴效应影响研究[J]. 情报学报, 2020, 39(4): 450-458.
- [2] 张敏, 郑伟伟. 基于信任的虚拟社区知识共享研究综述[J]. 情报理论与实践, 2015, 38(3): 138-144.
- [3] EVANS M M. Knowledge sharing: an empirical study of the role of trust and other social-cognitive factors in an organizational setting [D]. Toronto: University of Toronto, 2012.
- [4] WANG H, MENG Y, WANG W. The role of perceived interactivity in virtual communities: building trust and increasing stickiness [J]. Connection Science, 2013, 25(1): 55-73.
- [5] WU J J, TSANG A S L. Factors affecting members' trust belief and behaviour intention in virtual communities [J]. Behaviour and Information Technology, 2008, 27(2): 115-125.
- [6] ABDUL-RAHMAN A, HAILES S. Supporting Trust in Virtual Communities [C] //Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000.
- [7] 刘佩, 林如鹏. 网络问答社区“知乎”的知识分享与传播行为研究[J]. 图书情报知识, 2015(6): 109-119.
- [8] 鄢章华, 滕春贤, 刘蕾. 供应链信任传递机制及其均衡研究[J]. 管理科学, 2010, 23(6): 64-71.
- [9] 张春阳, 梁启华. 动态视角下人际信任对隐性知识共享意愿的影响研究——基于认知幸福感的中介效应[J]. 知识管理论坛, 2018, 3(6): 345-352.
- [10] 王鹏, 朱方伟, 宋昊阳, 鲍晓娜. 人际信任与知识隐藏行为: 个人声誉关注与不确定性感知的联合调节[J]. 管理评论, 2019, 31(1): 155-170.
- [11] 刘迎春, 谢年春, 李佳. 虚拟学习社区中基于用户行为的知识贡献者信誉评价研究[J]. 现代情报, 2020, 40(3): 117-125.
- [12] 洪亮, 冉从敬, 吴志强, 等. 基于用户声誉的数字图书馆知识社区资源管理机制研究[J]. 图书情报知识, 2014(6): 107-114.

## 作者简介

胡昌平, 男, 1946年生, 教授, 博士生导师, 研究方向: 信息资源管理理论、数字化信息资源管理与服务, E-mail: hcpwhu@163.com。  
李青青, 女, 1998年生, 硕士研究生, 研究方向: 数字信息资源管理。  
吕美娇, 女, 1987年生, 博士研究生, 研究方向: 信息资源管理与服务。

## Security Analysis of User Trust in Network Knowledge Community

HU ChangPing LI QingQing LV MeiJiao

(School of Information Management, Wuhan University, Wuhan 430072, China)

**Abstract:** This paper puts forward the countermeasures and suggestions to improve the supervision of user trust security in network knowledge community, which is to promote the governance of user trust security environment and provide reference for dealing with the security risk of user trust transmission. Through the investigation of trust transfer security in network knowledge community service, this paper analyzes the security risk factors in trust transfer. Based on this, aiming at the problems of users' trust preference, authentication management lag, malicious users' misleading, untrusted third party and the influence of service chain, the security guarantee of trust transmission in network knowledge community is improved; At the same time, from aspects of unifying knowledge community security evaluation standards, improving the user identity authentication system, establishing malicious user punishment rules, strengthening the supervision of the third party identification, this paper put forward suggestions to solve the influence of unsafe factors and trust security risk management and control measures.

**Keywords:** Network Knowledge Community; Trust Management; Security Guarantee

(收稿日期: 2021-04-01)