

# 电信诈骗如何导致误信： 影响因素、解释理论及研究展望

陈红敏<sup>1</sup>，赵雷<sup>2</sup>，郭素然<sup>3</sup>，莫雷<sup>4\*</sup>

(1.首都师范大学 马克思主义学院,北京 100048;2.中国青年政治学院 青少年工作系,北京 100089;  
3.国际关系学院 心理研究服务中心,北京 100091;4.华南师范大学 心理学院/  
心理应用研究中心,广州 510631)

**【摘 要】**电信诈骗严重影响社会信任,但探讨人们如何误信电信诈骗的心理机制的研究还比较欠缺。从电信诈骗受害者的角度分析电信诈骗误信的影响因素,发现受害者的电信诈骗易感性、诈骗者的社会影响技术以及受害者被骗时的心理状态起着关键的影响作用。对此,详尽可能性模型、骗子说服技巧模型和网络受骗易感性工作模型对现有研究进行了解释,但并不完善。未来的研究可以在模型的整合与发展、电信诈骗分类型分阶段研究的丰富和完善、因果研究方法的改进与创新、预防研究的实证性和可操作性方面深入开展。

**【关 键 词】**受害者 电信诈骗 易感性 误信 心理机制

**【中图分类号】**B842 **【文献标识码】**A **【文章编号】**1000-5455(2023)02-0094-13

## 一、引 言

电信诈骗指犯罪分子通过电话、网络和短信方式,编造虚假信息,设置骗局,对受害人实施远程、非接触式诈骗,诱使受害人给犯罪分子打款或转账的犯罪行为<sup>[1]</sup>。公安部数据显示,2021年1月至9月,全国共破获电信网络诈骗案件26.2万起,抓获犯罪嫌疑人37.3万名,同比分别上升41.1%和116.4%<sup>[2]</sup>。电信诈骗严重影响人民群众合法权益,不仅给人们造成财产损失,而且影响身心健康。欧盟开展的一项调查发现,24%的受害者在经济上遭受损失,79%的电信诈骗受害者在感情上遭受痛苦<sup>[3]</sup>。

电信诈骗若要获得成功,最关键的是要取得受害者的信任<sup>[4]</sup>。诈骗者通过网络和电信工具远程接触潜在受害者,如果没有受害者的参与和发挥积极作用(提供个人信息、汇款、对活动保密且不向执法部门报告),大部分骗局会失败。因此,揭示电信诈骗受害者误信的影响因素及心理机制,发现受害者误信的关键心理特征以及如何与电信诈骗情境互动的作用机制,对于保护潜在受害者、制定有效的预防电信诈骗策略和方

收稿日期: 2022-12-24  
基金项目: 国家社会科学基金一般项目“电信诈骗信任度的影响因素、心理机制及干预研究”(17BSH152)

通讯作者: 莫雷, E-mail: molei@senu.edu.cn

案至关重要。

## 二、电信诈骗误信形成的影响因素及研究

电信诈骗的形成是受骗者在诈骗者营造的诈骗情境的影响下,逐渐建立对诈骗者信任的过程。这一过程是诈骗者营造的诈骗情境和受骗者自身特征相互作用的结果。通过对已有研究的梳理分析发现,受骗者的电信诈骗易感性、诈骗者的社会影响技术以及受骗时受害者的心理状态均会影响人们对电信诈骗的误信。

### (一)受害者的电信诈骗易感性

Button 等人的研究表明,一小部分人似乎面临着被诈骗者重复欺骗的风险<sup>[5]</sup>。哪些人更容易受电信诈骗的影响?消费者行为、说服和决策相关的研究表明,个体差异可能会影响电信诈骗行为的易感性。

#### 1.受害者个人信息:人口统计学特点和信息泄露

相当多的研究分析了电信诈骗受害者的人口统计学特点,发现受害者的年龄、性别、受教育程度和收入等都是可能的影响因素,但还没有统一的结论<sup>[6]</sup>。虽然,目前的研究并没有提供关于受害者的人口统计学特点与诈骗易感性之间关系的清晰阐述,但可以确定的是,不同类别群体(男性与女性、年轻与年老等)误信电信诈骗与骗局有关:女性更有可能成为抽奖骗局的受害者,而男性更有可能成为彩票骗局的受害者;老年人更有可能成为投资诈骗的牺牲品,而年轻人则更容易成为在家工作和商业诈骗的受害者;离异和单身人士更易成为情感类诈骗的受害者等<sup>[5,7]</sup>。诈骗者正是根据受害者的年龄、性别等特点分析其需要,进行“精准推送”。此外,除了性别、年龄等人口统计学变量,个人其他信息的泄露也是导致个体受骗的主要原因,很多受害者表示当冒充权威身份的诈骗者精确地说出自己的姓名、身份证号、贷款或购物等信息时,自己很快信任了对方<sup>[6,8]</sup>。

#### 2.受害者的个性特点:高信任倾向和高风险偏好

受害者的信任倾向起着关键的影响作用,它是外部因素影响电信诈骗初始信任建立的重要结合点。信任倾向是一种人格特点,指个体在对他人没有任何已知信息的情况下所固有的信任水平<sup>[9]</sup>。它使人们能够高效处理每天接收的大量信息,但也给诈骗者提供了可乘之机。电信诈骗质性研究分析发现,个体信任倾向水平越高,越容易形成对他人和团体的信任<sup>[10]</sup>。Langenderfer 和 Shimp 认为,在受骗过程中,受害者可能关注的是人际互动,而不是与诈骗者对话的内容,他们相信诈骗者表面上的可信赖性(如身份),而不是认识到提供的内容不可信——根据经典沟通理论,他们关注的是信息的来源(人)而不是信息本身<sup>[4,11]</sup>。最新数据表明,冒充电商物流客服、公检法及政府机关工作人员、熟人、领导诈骗的案发量进入中国 2021 年前十大诈骗排名<sup>[12]</sup>。研究发现,受害者在电信诈骗受骗过程中与诈骗者建立信任时,基于两个条件:一是对熟人的信任度高,二是对权威的信任度高<sup>[13-14]</sup>。

风险偏好也会影响电信诈骗易感性。人们可以将电信诈骗视为非正式的彩票或赌博,风险偏好在应对中发挥重要作用。Anderson 的调查结果表明,与风险承受能力

低的人相比,风险承受能力高的个体报告的遭受诈骗的可能性几乎是其两倍<sup>[15]</sup>。Mueller 等人和 Wood 等人采用不同的方法,要求被试说出他们认为骗局提供的好处和风险。两项研究结果一致表明,被试的利益和风险认知是回应骗局邀请的主要预测因素<sup>[16-17]</sup>。未来的研究可以通过操纵利益和风险的大小,考察个体对风险和利益的认知是否有助于减少或增加对诈骗请求的反应意图。除此之外,已有研究还发现,具备诸如反社会、边缘型、依赖型人格障碍等人格特点的大学生更易成为诈骗受害者高危人群<sup>[18]</sup>。

### 3.受害者的认知特点:低认知能力和直觉思维方式

已有研究发现,认知能力和网络安全识别能力都对受骗有直接的影响。Crystal 等人的研究发现,认知能力降低对老年人受骗有直接的影响,轻度认知能力下降与诈骗易感性高相关,而中度至重度认知能力下降与诈骗易感性低相关,这可能是因为认知能力下降使个体理解诈骗企图变得困难<sup>[19]</sup>。就 75 至 89 岁的老年人来说,高认知能力是防止其成为“网络钓鱼”攻击牺牲品的保护因素<sup>[20-22]</sup>。网络安全识别能力越高的人越不容易受“网络钓鱼”骗局的影响<sup>[23]</sup>。但也有研究发现,一般受害人很难通过自身金融专业能力将精密骗局完全识破,一旦对骗局信任之后,网络自我效能感和网络安全识别能力高的特点也可能会成为其分享欺诈信息行为的“助推器”,导致被分享信息的人成为下一个电信诈骗的受害者,表现出“聪明反被聪明误”<sup>[24]</sup>。

在针对 90 后青年受害者的质性分析中发现,直觉思维方式也与诈骗中信任的形成密切相关<sup>[10]</sup>。思维双加工理论认为,人有两种不同的思维方式:直觉思维和分析思维。直觉思维不需要太多的意识和认知努力,是自动化的;分析思维更多依据规则进行分析思考,需要较多的认知资源和意识参与。兰楠和 Erik 等人的研究表明,在直觉式系统和分析式系统竞争时,个体在决策过程中会出现非理性偏差(认知繁忙、调整不足、直觉信心),而这些偏差正是导致直觉式系统在同分析式系统竞争中占优势的原因<sup>[25-26]</sup>。在诈骗者提供的诈骗情境中,个体基于诈骗者提供的信息和情境做决策时,可能会诱发较强的直觉信心,不会调动充足的认知资源进行分析思考,而采用直觉思维快速作出判断,导致误信诈骗者,进而增加上当受骗的可能性。此质性研究推理还需进行量化研究的验证。

## (二) 诈骗者的社会影响技术

与其他诈骗不同,电信诈骗不能通过面孔特征、表情、肢体语言等信息辅助进行判断,诈骗者只能在“隔空”的交往中通过编造虚假信息、建构虚假身份,以达到获取受害者信任,诱骗、欺骗、操纵受害者提供机密信息和资金的交际目的<sup>[27]</sup>。诈骗者编制的骗局、采用的骗术是影响个体对电信诈骗误信的主要诱发原因。

### 1. 编制的骗局

欺骗是成功诈骗的核心<sup>[4]</sup>。从受害者心理角度,电信诈骗骗局分为利益诱惑型(中奖、发补贴等)、避害心理型(冒充公权力机关涉嫌犯罪、银行卡消费、电话欠费、黑社会虚构绑架等)、情义救助型(冒充熟人求助、捐款等)、情感投资型(“杀猪盘”)等<sup>[28]</sup>。本研究总结发现,骗局主要包括两类内容:一是伪造“意外获得”,编造人们可

以意外获得巨额钱财信息,如中奖、粉丝福利、无息贷款等,用虚假的高收益驱使人产生高动机<sup>[14]</sup>;二是编造“意外事件”,编造突发的意外情境或紧急状况,如冒充公检法执法、家人出事、朋友需要紧急援助等,使人们在情急或应激状态下产生误判。

2. 使用的骗术

诈骗者通过诱骗个体执行不安全的行为,如打开含有恶意程序的电子邮件附件,或说服人们泄露自己的帐户和密码等,来实施诈骗。诈骗者实施的误导个体信任的技术被称作骗术<sup>[29]</sup>。例如,“网络钓鱼”电子邮件诈骗通过伪装成受信任的组织或机构联系个人<sup>[30]</sup>,引诱受害者点击邮件里看似合法的标识和网站链接<sup>[31]</sup>。为了让人们相信骗局的真实性,诈骗者通常采用一些社会规范技术,包括互惠技术(如提供礼物或优惠,使人们感到应该做出回应)、从众(如参考其他人的行为,使人们感到有顺从的压力)或权威性(如使用权威身份,让人们认为有义务遵守)<sup>[32-33]</sup>。此外,向潜在受害人灌输紧迫感也很常见,通过设定最后期限让个体尽快做出决定,而不能进行严谨的思考<sup>[10,34]</sup>。诈骗者有时也会唤起受害者的同理心和相似性,导致受害者相信诈骗者与他们有相同的期望和目标<sup>[35]</sup>。这些说服技术是否有效,一方面取决于个体是否对信息内容进行深入、系统的思考,另一方面也受到信息本身设计的影响<sup>[36]</sup>。表 1 为诈骗者常用的骗术。

表 1 电信诈骗中常见的骗术

| 骗 术           | 在电信诈骗中的应用                  |
|---------------|----------------------------|
| 权威            | 冒充权威人物或机构,如警察、银行或高级人员      |
| 讨人喜欢的形象或资料    | 创建描绘可信赖特征或显得友好的个人资料        |
| 从众            | 暗示其他人已受益                   |
| 承诺和一致性(登门槛效应) | 先要求支付少量预付费用(如预付费欺诈),后提出高要求 |
| 互惠            | 提供免费礼物或恩惠                  |
| 紧迫感           | 设置时间限制                     |
| 奖励            | 承诺金钱或心理上的奖励                |
| 损失            | 声称不回复将导致某种损失,如“账户关闭”       |

(三)受害者被骗时的心理状态

电信诈骗误信何时形成与受害者被骗时的心理状态紧密相关。具体来说,诈骗者通过谎称的信息唤醒受害者高需求动机或者高情绪状态而影响个体的信任,具有不同自我特征的个体对骗局的反应不同。

1. 被诱发的心理动力:动机与情绪

从电信诈骗受害者决策和判断的心理动力特征分析,有研究将其归为两种路径:“弱势-信任”模式和“趋利-避害”模式。前者是诈骗者利用受害者的弱势心理向其传递虚假信息,达到受害者“自愿”转账付款的目的;后者认为受害者的心理特征可以分为趋利心理和避害心理,诈骗者在取得信任之后利用这两种心理需求对受害者进行操纵,从而获利<sup>[24]</sup>。而这背后深层次的原因是,通过虚假信息诱发受害者趋利或避害的高动机。当人们处于强烈的动机状态时,决策和处理相关信息的质量会降低,更容易信任诈骗者<sup>[14]</sup>。研究者对 111 封“尼日利亚诈骗信件”的内容进行分析,发现邮件中的关键成分是“意外之财”的叙事故事吸引了潜在受害者强烈的情感,这些信件诱发贪

婪、慈善、英雄主义和其他相关的强烈情感线索”<sup>[35]</sup>。另一项研究表明,30%的受害者报告了他们措手不及,13%的受害者提到期待得到一笔好交易或赢得奖品的兴奋<sup>[37]</sup>。

在信息加工的过程中,情绪也会影响信任。Bower的研究发现,情绪会通过检索与记忆中情绪一致的信息来影响判断<sup>[38]</sup>。而Martin等人则发现,个体自身情绪会影响情绪与信任之间的关系<sup>[39]</sup>。即,当某个人采取某种特殊的行动,是因为他们被激励去采取这种行动,并把这种行动用来维持或者修复现有的一种情绪状态。Dunn和Schweizer在研究中发现,正面情绪会增加信任,而负面情绪则会减少信任<sup>[40]</sup>。有研究发现,无论是老年人还是年轻人,高唤醒的积极情绪或消极情绪相较于没有情绪唤醒,都显著增加了被试购买虚假广告商品的意愿;不管老年人的情绪唤醒情况如何,他们报告的购买意愿比年轻人更强<sup>[41]</sup>。一项针对疫情期间诈骗的研究也发现存在情绪的影响,对新冠病毒的恐惧正向预测对新冠病毒特定主题的“网络钓鱼”骗局的成功,而焦虑、压力水平对新冠疫情和普通“网络钓鱼”骗局的成功都有正向预测作用<sup>[42]</sup>。

## 2. 与自我相关的因素

通过分析以往的研究发现,受害者自我意识、自我控制高低等特点也会影响受害者与电信诈骗情境互动的易感性。当个体认为自己与诈骗信息中的主角相似时,这种自我意识会增加受骗易感性,如曾遭遇过苦难的人对有说服力的慈善募捐类的电信诈骗骗局的敏感性会增加;个体只有在认为自己与诈骗信息主角不同时,才会表现出更强的抵抗力<sup>[43]</sup>。研究者对11 000多名互联网用户的分析发现,自我控制成为网络诈骗受害者的关键预测因素<sup>[44]</sup>。一项针对新冠疫情骗局易感性的年龄差异和个体差异的结果表明,受骗易感性可能是低自我控制的结果,表现为冲动且不易被抑制,甚至不受过去受骗经验的影响<sup>[45]</sup>。Baumeister通过影响人们长期目标的行为能力发现,影响自我控制的两个主要因素是标准(个人价值观和理想)和监测(对个人行为的意识和跟踪),说明自我控制和诈骗易感性之间的关系可以通过自我意识来调节<sup>[46]</sup>。自我耗竭和目标冲突也被认为与自我控制负相关,因此,没有明确一致的目标、情绪低落或没有足够的心理力量来克服冲动的人,更容易出现自我控制失败和在电信诈骗中受影响。

# 三、电信诈骗误信的心理机制及相关理论

## (一) 详尽可能性模型

详尽可能性模型(Elaboration Likelihood Model)通过阐释受害者受骗时被诱发的强烈心理动力的信息加工机制,来解释受害者“何时”误信的问题。详尽可能性模型最初被用来解释个体的态度是如何通过两条说服路径(中心路径和外围路径)发生改变的<sup>[47]</sup>。中心路径信息加工需要大量思考,因此需要高度精细化。相反,外围路径信息加工不涉及精细化,并且个体可能会关注来源的吸引力。使用中心路径处理信息的个体因为信息很重要,所以有动力使用足够的认知资源;而采用外围路径的个体出于个人原因或因信息量较少而使用。借鉴这个模型,Rusch认为,诈骗者通过诈骗信息激起强烈的情绪,如兴奋或恐惧,导致个体没有太多的认知资源而只能依靠外围路径进行

加工<sup>[48]</sup>。Langenderfer 和 Shimp 在一篇理论文章中也认为, 诈骗信息唤起了受害者的贪婪等高动机需求(如赚大钱), 动机强烈的个体更容易忽略信息中提醒他们注意骗局的线索, 而把更多的注意力放在中奖等信息方面<sup>[4]</sup>。个体越关注奖励, 非奖励信息获得的加工就越少。因此, 当骗局中奖励越高时, 高情绪且高动机的个体越容易被欺骗<sup>[49]</sup>。相比之下, 当个体不关注奖励信息时, 更容易识别骗局, 避免被骗。这一理论解释不仅在实验研究中得到了验证, 在干预研究中也得到了验证<sup>[41,50]</sup>。详尽可能性模型从信息加工的角度关注诈骗者的说服技巧是如何启动受害者的外围加工路径以达到说服受害者误信的目的, 对受害者误信的影响因素之一“被诱发的心理动力——情绪和动机”的心理机制进行了很好的阐释, 对个体为什么受大规模营销诈骗这一问题有一定的解释作用。但该模型并没有对电信诈骗的形成过程进行解释, 也没有清晰地指出内外部影响因素在电信诈骗误信中的作用。

(二) 骗子说服技巧模型

骗子说服技巧模型(The Scammers Persuasive Techniques Mode)是 Whitty 通过对网络约会浪漫骗局 20 位受害者的深入访谈后提出的六阶段发展模型(见图 1)<sup>[51]</sup>。该图解释了个体如何误入骗局并最终被骗取钱财的过程。

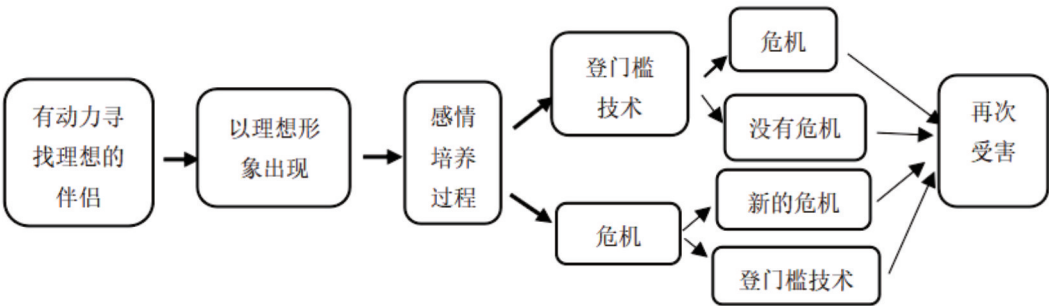


图 1 骗子说服技巧模型

第一阶段, 潜在受害者在网上寻找理想伴侣, 他们均为单身或者离异。第二阶段, 骗子向潜在受害者提供虚假的信息, 根据潜在受害者寻找伴侣的典型特征, 将自己伪装成潜在受害者的理想对象。伪装的男性形象通常是丧偶、带孩子、从事专业工作或商人。伪装的女性形象可能是穷学生或者从事低收入工作的人。研究人员发现, 女性倾向寻找社会经济地位高的伴侣, 而男性倾向寻找外表有吸引力的伴侣<sup>[52]</sup>。第三阶段, 培养感情阶段。骗子为受害者提供一个看似安全的环境, 让他们吐露心声或秘密, 获得受害者的信任。第四阶段, 欺骗阶段。在这一阶段, 骗子通过登门槛技术和危机事件技术, 主动提出金钱的要求。所谓登门槛技术, 就是骗子向受害者索要礼物或少量金钱作为一种尝试, 如果受害者顺从, 骗子便会不断地要更多的钱。危机事件技术指骗子向受害者发出求助信息, 如谎称发生了交通事故或遭到抢劫, 请受害者垫付医疗费或向受害者借钱。如果受害者与骗子感情培养得好, 受害者信任了骗子, 便会给钱; 如果没有, 受害者会试图退出这段关系, 这时骗子会回到第三阶段, 继续培养感情。一些受害者在此阶段中断联系, 成功逃离骗局。第五阶段, 对于那些在危机事件中没有顺从的人, 骗子采用“以退为进”技术, 继续向受害者编造新的危机事件或小额资金

请求,直到受害者耗尽资金或退出骗局。第六阶段,即使受害者被执法部门告知其正在受骗,他们又会回到同一个骗局或又进入新的骗局<sup>[53]</sup>。该模型认为,浪漫骗局的受害者会对这个骗局上瘾,但这一领域需要更多的研究来进一步证实<sup>[54-55]</sup>。骗子说服技巧模型是一种特定诈骗类型的全过程模型,此模型对于解释网络恋爱骗局的发展阶段和说服技巧有一定的意义和价值,如对“杀猪盘”骗局有一定的适用性<sup>[28]</sup>。但该模型不能解释电信诈骗中其他类型的骗局,对电信诈骗不具有普遍适用性,并且也没有清晰揭示影响电信诈骗误信的主要因素及其相互作用机制。

(三) 网络受骗易感性工作模型

为了让人们充分理解受害者个体差异、情境因素和骗子提供的影响信息之间相互作用的关系,有研究者提出了网络受骗易感性工作模型<sup>[56]</sup>。该模型的提出是为了构建一个网络诈骗的情境,在该情境下研究骗子和受害者之间的相互交往、受害者的处境以及发生的影响机制,以期为未来的研究提供理论框架。在这个模型中,个体的受骗易感性被分为四个层面的影响因素,分别是“谁”“何时”“何地”“发生了什么”。具体来说:

“谁”:接受者的个人特征,如个性和风险偏好;

“何时”:接受者当前的状态,如他们当前的情绪、自我意识的程度、认知压力或疲劳;

“何地”:个人当时所处的环境,如他们是在家还是在工作,使用的交流媒介以及更广泛的文化价值观的影响;

“发生了什么”:所使用的骗术,如唤起遵从权威、激发时间压力或诱发特定的情绪(如恐惧、兴奋等)。

这些因素在任何既定的时间点都可能影响个人对电信诈骗的易感性。该模型认为,以上每个层面弱点的存在都会导致个体受骗易感性的增加,因此,具有特定弱点的人在脆弱的环境中比在中性环境中更容易受到影响。由于骗术是为了利用个人或情境层面的特定弱点专门设计的,骗子发布的含有骗局和骗术的信息与这些弱点进一步交互作用,对个体的受骗易感性产生更大的影响。模型假设,从总体上说,这四个方面累加到一起,是一个相对线性的、可加性的效应,公式如下:

$$\text{个体受骗易感性} = \text{接受者的个人特征} + \text{接受者的当前状态} + \text{接受者当时所处的环境} + \text{所使用的骗术}$$

当然该模型也强调,某些因素组合对易感性具有指数效应,而不是线性效应。

图 2 列举了每一层面关键的影响因素,该模型可以应用到各种诈骗类型中并进行拓展。图中灰色阴影部分表明受害者在工作场所遭遇“网络钓鱼”攻击,每一层面的哪些关键因素如何相互作用的示例。例如,一个对隶属关系有高度需求的员工可能会优先考虑在工作场所内维持和谐的关系。当在疲劳或认知超负荷的情况下,所处职位的权力或地位相对较低的员工,特别容易受到骗子操纵(利用)的互惠、权威或从众企图的影响(见图 2 中的阴影框)。



图 2 基于工作场所“网络钓鱼”攻击的个体受骗易感性模型的假设框架

网络受骗易感性工作模型从电信诈骗影响因素的横切面视角分析受害者受骗敏感性的叠加效应,对解释电信诈骗中“谁、为何以及何时选择信任”有非常重要的作用,对电信诈骗骗局有一定的适用性。该模型对本研究第二部分中的影响因素有很好的解释力,但也仅能解释部分因素,而对受害者面对电信诈骗时内外部因素如何交互作用的深层心理机制不能详细说明。此外,该模型还缺少对电信诈骗误信形成的动态变化过程的解释力<sup>[57]</sup>。

四、研究展望

综上所述,国内外关于电信诈骗误信的研究虽然成果颇丰,但也存在一些局限。其一,从理论阐释来看,已有的理论一部分聚焦某种特定电信诈骗类型,另一部分围绕电信诈骗的某个环节,还有一部分从影响因素的横切面进行解释,现有理论无论在适用性还是在解释力上都有提高的空间。其二,从研究内容来看,目前学界对电信诈骗信任影响因素的研究,往往只是孤立地探讨某个外在因素(扮演身份、骗局)或内在因素(个体原因),抑或某些电信诈骗的具体环节,研究还缺乏系统性和整体性。实际上,电信诈骗之所以成功获得人们信任,是因为该过程往往存在复杂的内外因素交互作用,应在研究外在因素时结合相关的个体内在因素来探讨。其三,从研究方法来看,目前的研究大多是用社会调查或者案例分析方法进行的回溯性分析,实验研究较少。基于社会调查所做的研究更多反映的是相关关系,不能准确探究诈骗与误信之间的因果关系。其四,从应用研究来看,电信诈骗研究的目的是有效应对和预防电信诈骗,目前该方面的经验范畴研究较多,实证研究较少,尤其缺少高质量的针对电信诈骗预防的干预实证研究。基于以上局限,未来的研究可以从以下四个方面进行拓展。

第一,模型的整合与发展。电信诈骗如何获取个体的信任是一个多层面、动态的问题。实际上,电信诈骗之所以成功获得人们信任,是因为该过程往往存在复杂的内外因素交互作用,即从初始信任到信任深入继而保持的过程。基于此,应在不同信任建立阶段研究外在因素与个体内在因素的交互作用。因此,本研究认为,可以建构出涵盖范围更广的、解释力更强的理论——电信诈骗信任形成的过程模型,动态、系统地阐释电信诈骗不同信任阶段的关键影响因素及其之间的作用机制。

该模型将电信诈骗信任分为两个阶段:快速信任阶段和信任维持阶段。在快速信任阶段,个人信息的泄露、骗子冒充的权威身份与个体的信任倾向相契合,导致个体快速进入初始信任。在信任维持阶段,诈骗者谎称的利益诱惑类或应急避险类骗局、“小恩小惠兑现的登门槛效应”“谎称他人行为示范的从众策略”和设置时间紧迫感等骗术,诱导出个体“趋利”或“避害”的高需求动机以及高负性 or 高正性情绪紧张状态,导致个体注意力狭窄、认知资源受限,最终只能采用基于直觉的启发式系统决策,从而产生非理性的决策偏差(见图3)。

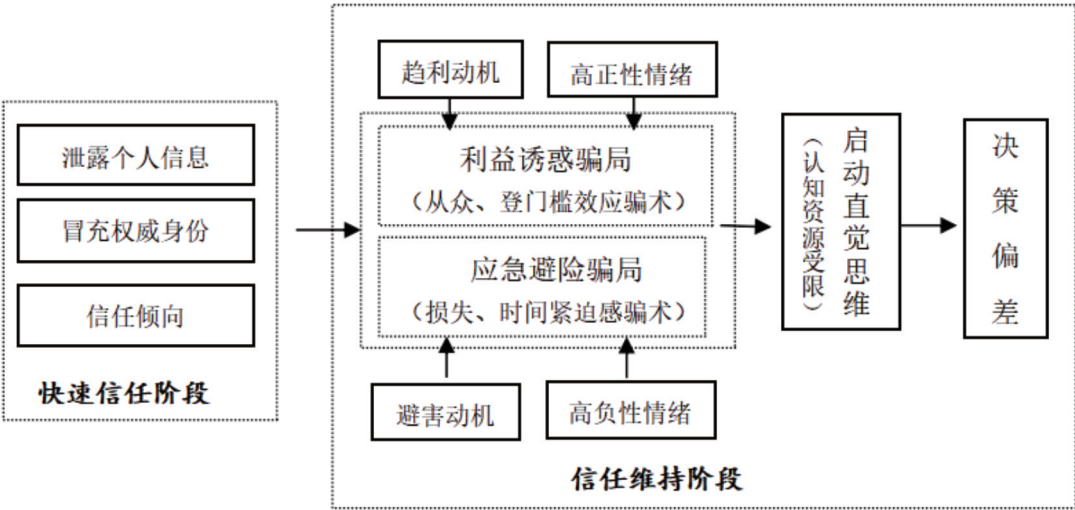


图3 电信诈骗信任形成的过程模型

第二,电信诈骗分类型分阶段研究的丰富和完善。未来的研究可以从以下三方面对研究内容进行丰富和完善。一是针对不同类型的电信诈骗,开展更具针对性的实证研究。已有的研究尽管将电信诈骗划分为不同的类型,但在实证研究中并没有特别关注不同类型的影响作用。未来的研究可以进一步细化电信诈骗类型,通过骗局类型(获得类、损失类)和冒充主体(熟人、陌生人、权威人士)的交互作用,精细化探讨不同电信诈骗类型中信任形成的影响因素和心理机制,并比较不同电信诈骗类型中信任形成的差异。二是聚焦电信诈骗信任形成的不同阶段,开展更加具体的实证研究。已有质性研究发现,电信诈骗的信任形成过程是一个分阶段、动态的过程,但缺乏针对具体信任形成阶段的实证研究。未来可以聚焦电信诈骗信任形成的某一具体阶段,探讨影响特定阶段信任形成的主要因素和机制,从而得出更有价值的研究结果。三是变量的拓展和整合。电信诈骗的形成是内外部因素共同作用的结果。已有的研究尽管围绕内外部影响因素做了大量探讨,并发现了许多重要的影响因素,但还有一些关键的因素,如个体意识、个人经验、气质类型、外界环境的阻断作用等探讨较少,未来的研究可以加强对这些因素的讨论。

第三,因果研究方法的改进与创新。以往研究主要采用回溯性分析,但基于回溯报告(调查问卷和公安犯罪统计)的研究可能存在报告偏差,更多受害者因无法识别骗局、羞愧或自责等不愿意报告受骗经历,如有研究发现仅有15%的受害者向当局报告了受骗经历<sup>[58]</sup>。未来的研究方法可以从以下三方面改进提高。一是强化实验研究方

法运用。未来应更多开展探讨因果关系的实验研究,以更好揭示电信诈骗信任形成的心理机制。二是创新实验范式,提升实验研究的内部效度和生态效度。一方面可以借鉴成熟的启动实验范式,通过启动被试的紧张情绪、分析思维等心理因素,更加准确地反映受害者在电信诈骗中的真实心理状态,从而提升研究的内部效度;另一方面要运用现场实验、计算机模拟等方法和技术,模拟创设更真实的电信诈骗情境,以期发现更具有生态效度的结果,发现更符合真实情境的规律和结论。三是运用多学科实验方法。除了目前常用的实验室实验等研究方法之外,也要借鉴多学科的研究方法,特别是要借鉴认知神经科学的研究技术和工具,找到电信诈骗对个体产生影响的神经生理基础。这些方法的应用将使电信诈骗对个体影响的研究更加科学化,也会产生更多有价值的成果。

第四,预防研究的实证性和可操作性。研究电信诈骗信任形成机制的实践目的是减少电信诈骗对人们的危害。有研究发现,预警可以降低易受攻击的消费者对于欺诈的敏感度<sup>[59]</sup>。Daiku 等人进一步的研究发现,被试在有预警并记住预警骗局的前提下,诈骗信息只有被个体通过中心路径而不是外围路径进行加工,预警才能起到作用<sup>[50]</sup>。这与已有研究发现个体的思维加工方式(直觉思维和分析思维)有相似之处<sup>[10]</sup>。还有研究发现,道德的提升可以增加个体的轻信<sup>[60]</sup>。尽管如此,电信诈骗预防的实证研究与基础研究相比相对较少,大多属于经验与常识范畴<sup>[6]</sup>,而具体提高个体诈骗识别能力的干预研究则更少。所以,未来还要进一步聚焦提高人们对电信诈骗的识别能力和预防能力的干预方案,并通过实验方法检验干预方案的有效性。

## 参考文献:

- [1] O'BRIEN J T. Telecommunications fraud[J]. Fbi law enforcement bulletin, 1998,67(5):2107.
- [2] 公安部.今年前9个月全国共破获电信网络诈骗案件26.2万起[EB/OL].(2021-10-26)[2022-10-19]. [https://s.cyol.com/articles/2021-10/26/content\\_r2vaw6h3.html](https://s.cyol.com/articles/2021-10/26/content_r2vaw6h3.html).
- [3] BIJWAARD D. Survey on "scams and fraud experienced by consumers" - final report [J/OL]. (2020-01-28) [2022-10-19]. <https://policycommons.net/artifacts/2135251/survey-on-scams-and-fraud-experienced-by-consumers/2890549/>.
- [4] LANGENDERFER J, SHIMP T A. Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion [J]. Psychology and marketing, 2001, 18(7): 763-783.
- [5] BUTTON M, LEWIS C, TAPLEY J. Fraud typologies and victims of fraud: literature review [R]. London: National Fraud Authority, 2009:40.
- [6] HANOCH Y, WOOD S. The scams among us: who falls prey and why [J]. Current directions in psychological science, 2021, 30(3):260-266.
- [7] WHITTY M T. Is there a scam for everyone? Psychologically profiling cyberscam victims [J]. European journal on criminal policy and research, 2020, 26(3):1-11.
- [8] 赵雷,陈红敏.电信诈骗中青年受骗的影响因素和形成机制研究[J].中国青年社会科学, 2022,41(3):102-112.
- [9] WU G, HU X, WU Y. Effects of perceived interactivity, perceived web assurance and disposition to

- trust on initial online trust [J]. *Journal of computer-mediated communication*, 2010, 16(1): 1-26.
- [10] 赵雷,黄雪梅,陈红敏.电信诈骗中青年受骗者的信任形成及其心理——基于9名90后电信诈骗受骗者的质性分析[J]. *中国青年研究*, 2020(3): 49-54.
- [11] HOVLAND C I, JANIS I L, KELLEY H H. *Communication and persuasion: psychological studies of opinion change* [M]. New Haven CT: Yale University Press, 1953: 355-357.
- [12] 2021年电信网络诈骗治理研究报告[EB/OL]. (2021-10-26) [2022-10-10]. <https://baijiahao.baidu.com/s?id=1714686420710721046&wfr=spider&for=pc>.
- [13] 唐丽娜,王记文.诈骗与信任的社会机制分析——以中国台湾跨境电信诈骗现象为例[J]. *学术论坛*, 2016, 39(5): 97-103.
- [14] FISCHER P, LEA S E, EVANS K M. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance [J]. *Journal of applied social psychology*, 2013, 43(10): 2060-2072.
- [15] ANDERSON K B. Mass-market consumer fraud in the United States: a 2017 update staff report [R]. Washington, DC: Bureau of Economics, Federal Trade Commission, 2019: 95-99.
- [16] EMILY A M, STACEY A W, YANIV H, et al. Older and wiser: age differences in susceptibility to investment fraud: the protective role of emotional intelligence [J]. *Journal of elder abuse & neglect*, 2020, 32(2): 152-172.
- [17] STACEY W, LIU P J, YANIV H, et al. Call to claim your prize: perceived benefits and risk drive intention to comply in a mass marketing scam [J]. *Journal of experimental psychology-applied*, 2018, 24(2): 196-206.
- [18] 许志炜,童泽林,郭显琅,等.诈骗受害大学生的人格特质[J]. *中国心理卫生杂志*, 2021, 35(9): 775-780.
- [19] CRYSTAL M G, YU L, CHRISTOPHER C S, et al. Childhood socioeconomic status interacts with cognitive function to impact scam susceptibility among community-dwelling older adults [J/OL]. (2022-06-13) [2022-10-11]. <https://www.tandfonline.com/doi/abs/10.1080/13607863.2022.2087206?journalCode=camh20>.
- [20] NATALIE C E, DONOVAN M E, LIN T, et al. Uncovering susceptibility risk to online deception in aging [J]. *The journals of gerontology series B-psychological sciences and social sciences*, 2020, 75(3): 522-533.
- [21] REBECCA A J, SARA N G, YANG L, et al. The role of cognition, personality, and trust in fraud victimization in older adults [J]. *Frontiers in psychology*, 2017, 8(3): 275-282.
- [22] MATTHEW D G, KATELYN S M, ZIAD M H, et al. Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails [J]. *The journals of gerontology series B-psychological sciences and social sciences*, 2020, 76(9): 1711-1715.
- [23] WRIGHT R T, MARETT K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived [J]. *Journal of management information systems*, 2010, 27(1): 273-303.
- [24] 李辉.电信诈骗情境下受害人欺诈信息接受意愿及其分享行为研究[J]. *图书情报工作*, 2021, 65(7): 90-102.
- [25] 兰楠.双加工理论的两系统在决策过程中的加工方式探讨[D].西安:陕西师范大学, 2018: 4-6.
- [26] ERIK D, KEVIN W R, MICHAEL G P. When should I trust my gut? Linking domain expertise to

- intuitive decision-making effectiveness [J]. *Organizational behavior and human decision processes*, 2012, 119(2): 187-194.
- [27] NING Y, LE C, YUN Z. Identity construction of suspects in telecom and internet fraud discourse: from a sociosemiotic perspective [J]. *Social semiotics*, 2019, 29(3): 319-335.
- [28] 向静, 刘亚岚. “杀猪盘”电信诈骗犯罪的心理控制机制剖析[J]. *中国人民公安大学学报(社会科学版)*, 2021, 37(4): 1-10.
- [29] ATKINS B, HUANG W. A study of social engineering in online frauds[J]. *Open journal of social sciences*, 2013, 1(3): 23-32.
- [30] GREITZER F L, STROZER J R, COHEN S, et al. Analysis of unintentional insider threats deriving from social engineering exploits [R]. San Jose, CA: IEEE Security and Privacy Workshops, 2014: 236-250.
- [31] WORKMAN M. Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security [J]. *Journal of the American society for information science and technology*, 2008, 59(4): 662-674.
- [32] DAVID M, LEA S. Scam compliance and the psychology of persuasion [J/OL]. (2013-01-01) [2022-10-19]. <http://ssrn.com/abstract=2364464>.
- [33] STAJANO F, WILSON P. Understanding scam victims: seven principles for systems security [J]. *Communications of the ACM*, 2011, 54(3): 70-75.
- [34] KLAPATCH L, HANOCH Y, WOOD S, et al. Consumers' response to mass market scam solicitations: profiling scams and responses[J]. *Psychology, crime, and law*, 2022, 2038599: 1-19.
- [35] CUKIER W L, NESSELROTH E J, CODY S. Genre, narrative and the “Nigerian Letter” in electronic mail[C]. Hawaii: Proceedings of the 40th annual Hawaii international conference on system sciences, 2007: 70.
- [36] XIAO B, BENBASAT I. Product-related deception in e-commerce: a theoretical perspective [J]. *MIS quarterly*, 2011, 35(1): 169-195.
- [37] GEORGE S. Research on impact of mass marketed scams[R]. London: Office of Fair Trading, 2006.
- [38] BOWER G H. Mood and memory [J]. *The American psychologist*, 1981, 36(2): 129.
- [39] LEONARD L M, DAVID W W, JOHN W A, et al. Mood as input: people have to interpret the motivational implications of their moods [J]. *Journal of personality and social psychology*, 1993, 64(3): 317-326.
- [40] JENNIFER R D, MAURICE E S. Feeling and believing: the influence of emotion on trust [J]. *Journal of personality and social psychology*, 2005, 88(5): 736.
- [41] KATHARINA K, NANNA N, MARGUERITE D, et al. Emotional arousal may increase susceptibility to fraud in older and younger adults [J]. *Psychology and aging*, 2018, 33(2): 325-337.
- [42] ABROSHAN H, DEVOS J, POELS G, et al. COVID-19 and 640 phishing: effects of human emotions, behavior, and demographics on 641 the success of phishing attempts during the pandemic [J], *IEEE Access*, 2021, 642(9): 121916-121929.
- [43] HUNG I W, WYER R S. Effects of self-relevant perspective-taking on the impact of persuasive appeals [J]. *Personality and social psychology bulletin*, 2014, 40(3): 402-414.
- [44] CHEN H, BEAUDOIN C E, HONG T. Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors [J]. *Computers in human behavior*, 2017, 70: 291-302.

- [45] JULIA N, YANIV H, STACEY W, et al. Susceptibility to COVID-19 scams: the roles of age, individual difference measures, and scam-related perceptions [J]. *Frontiers in psychology*, 2021, 12: 789883.
- [46] BAUMEISTER R F. Ego depletion and self-control failure: an energy model of the self's executive function [J]. *Self and identity*, 2002, 1(2): 129-136.
- [47] JOHN T C, RICHARD E P, et al. The need for cognition [J]. *Journal of personality and social psychology*, 1982, 42(1): 116-131.
- [48] RUSCH J J. The "social engineering" of internet fraud: internet society annual conference [EB/OL]. (2003-12-14) [2022-10-19]. [http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm).
- [49] NORRIS G, BROOKES A. Personality, emotion and individual differences in response to online fraud [J]. *Personality and individual differences*, 2021, 169: 109847.
- [50] YASUHIRO D, NAOKI K, TSUKASA T, et al. Effective forewarning requires central route processing: theoretical improvements on the counter argumentation hypothesis and practical implications for scam prevention [J]. *PloS one*, 2020, 15(3): e0229833.
- [51] WHITTY M T. The scammers persuasive techniques model [J]. *British journal of criminology*, 2013, 53(4): 665-684.
- [52] KENRICK D T, SADALLA E K, GROTH G, et al. Evolution, traits, and the stages of human courtship: qualifying the parental investment model [J]. *Journal of personality*, 1990, 58(1): 97-116.
- [53] SORELL T, WHITTY M. Online romance scams and victimhood [J]. *Security journal*, 2019, 32(3): 342-361.
- [54] WHITTY M T. Do you love me? Psychological characteristics of romance scam victims [J]. *Cyber psychology, behavior and social networking*, 2018, 21(2): 105-109.
- [55] WHITTY M T. Predicting susceptibility to cyber-fraud victimhood [J]. *Journal of financial crime*, 2019, 26(1): 277-292.
- [56] WILLIAMS E J, BEARDMORE A, JOINSON A N. Individual differences in susceptibility to online influence: a theoretical review [J]. *Computers in human behavior*, 2017, 72: 412-421.
- [57] 赵竞, 孙晓军, 周宗奎, 等. 网络交往中的人际信任 [J]. *心理科学进展*, 2013, 21(8): 1493-1501.
- [58] TITUS R M, GOVER A R. Personal fraud: the victims and the scams [J]. *Crime prevention studies*, 2001, 12: 133-151.
- [59] SUSANNE S, NANNA N, JOSEPHINE M, et al. Forewarning reduces fraud susceptibility in vulnerable consumers [J]. *Basic and applied social psychology*, 2014, 36(3): 272-279.
- [60] ANNE H, BRENT M, DARREN W D. Above the scam: moral elevation reduces gullibility [J]. *Journal of consumer psychology*, 2021, 32(3): 466-474.

【责任编辑:王建平,助理编辑:何婉婷;责任校对:王建平】