Chapter

3 第3章

社工黑客的常用直接攻击

学习目标

- 了解欺骗的三要素和分类法
- 了解构成欺骗的必要条件，尤其要了解骗子经常营造的行骗环境等
- 熟悉骗子行骗的着力点和主要方法，掌握骗子的意识操控和信息操控等方法
- 掌握良好伪装的九大基本原则和四个重要特性
- 熟悉谣言、谎言与流言的特点、传播、识别与辟谣
- 掌握有关态度改变的主流理论
- 熟悉说服的主要模型，掌握影响说服效果的因素和说服的实用技巧
- 了解动机与行为的关系
- 了解需求与诱惑的关系
- 熟悉社工的常见诱惑手段
- 了解社工黑客操控他人的主要规则

案例导入

社工黑客的几乎所有攻击行为都或多或少地涉及欺骗，故有关欺骗的可选案例非常多。不过，我们只介绍一个由“世界头号黑客”米特尼克讲述的曾被《吉尼斯世界纪录大全》评为“最大的计算机诈骗”的真实案例。该故事的主角名叫瑞夫金，他是米特尼克崇拜的社工黑客偶像之一。

话说，1978 年的瑞夫金还只是某公司的安全工程师。当时，他受命前往太平洋实业银行承建一个安全系统，以便应对可能发生的安全事件。于是，他借机熟悉了该行的转账过程，更知道每天早晨该行都会将当日有效的操作口令临时告知电汇室核心人员，供他们在

打电话汇款时验明正身，避免被假冒。可是，由于口令更换过于频繁，电汇员们害怕混淆，就自作聪明地将当日口令写在桌面的纸条上，这让瑞夫金乐得合不拢嘴。

经过一段时间的精心准备后，瑞夫金的社工攻击开始了。一天，他以维护安全系统的名义，早早来到银行，假装忙忙碌碌地埋头苦干，双眼和双耳当然都没闲着。果然，他很快就如愿以偿地记下了当日的操作口令，并转身离开电汇室。大约当天下午 3 点，瑞夫金以该行国际部经理汉森的身份，通过街边公共电话拨通了电汇室的电话。

“喂，是电汇室吗？我是国际部的汉森”，他对接电话的电汇员说道。

电汇员按标准程序询问了他的办公室号码。“286 房间”，瑞夫金胸有成竹地按预定剧本回答道。

接着，电汇员问出了那个最关键的问题：“今天的操作口令是什么？”

早已因害怕露馅而心跳不已的瑞夫金，仍然平静地答道：“4789。”然后，他熟练地给出了转账指令“请转 1020 万美元到瑞士×××银行的×××账号”，其实该账号是瑞夫金在前几天专门为自己开设的账户。

本以为已经马到成功的瑞夫金怎么也没想到，那位电汇员又突然问出了另一个意外问题：“好的，我马上汇款。另外，请问电汇室的跨部门授权号是什么？”

瑞夫金一听就傻眼了，他压根儿就不知道还需要跨部门授权号这件事。幸好，他一边直冒冷汗，一边赶紧机智地答道：“请稍等，我一会打电话给你!”

放下电话后，他又摇身一变，以电汇员身份给银行的另一个部门打电话。果然，对方很熟练地就告诉了他电汇室的跨部门授权号。于是，刚才那位负责转账的电汇员经过一番熟练操作后，满足了瑞夫金的要求。

几天后，瑞夫金飞到瑞士，取出了现金，买回了一堆钻石，从而不费吹灰之力就创造了一项吉尼斯世界纪录。

第 1 节　欺骗的一般规律

学习提示

- 了解欺骗的三要素，以及分类方法。
- 熟悉构成欺骗的必要条件以及骗子营造的欺骗环境。
- 熟悉骗子的一些常用面具，以便更好地识破和对付骗子。
- 熟悉骗子行骗的着力点和主要方法，以及骗子的意识操控和信息操控等方法。
- 了解骗子为了营造假象所进行的隐瞒、选配、作假、曲解、颠倒等信息操控方法，以及若干意识操控方法。

如何面对各种可能的欺骗，这是一个问题。如果我们过于单纯，认为世界很美好，那就很容易成为骗子的牺牲品。如果我们过于担心自己可能会被他人欺骗，从而随时保持高度警惕，随时怀疑一切，那我们的日子将备受煎熬。不过，作为网络安全领域的从业人员，为了对付无处不在的社工黑客，我们有必要适当了解欺骗的一些基本知识。

关于“欺骗”的定义，你只需意会，不必去言传，因为翻开任何一本词典，你不仅可以查到“欺骗”的释义，而且还可以找到众多与“欺骗”意义相近的词，比如：《现代汉语词典》第 7 版中，对“欺骗”释义为“用虚假的言语或行动来掩盖事实真相，使人上当”；其意义相近的词有欺诈、诱惑、迷惑、哄骗、愚弄、瞒哄、诓骗、诈骗、障眼、戏弄、开涮、诱骗、诓人、尔虞我诈、狡诈、伪善、逢迎、诋毁、诽谤、讹诈、耍花招、摆噱头、作假、耍奸、耍滑头、弄虚作假、欺上瞒下、上当受骗、瞒天过海、挂羊头卖狗肉、妖言惑众、故弄玄虚、迷人眼目、偷梁换柱、偷天换日、弄鬼、做手脚、浑水摸鱼等。

这里研究欺骗的目的，当然不是教唆大家去行骗，而是要提醒大家识别欺骗和反欺骗。所谓欺骗，是一种社会行为，它通过捏造事实或掩盖真相，达到某种预期目的。更具体地说，欺骗具有三要素：

（1）虚假性。从真伪角度看，欺骗的突出特点是“伪”，即捏造事实，或者掩盖事实真相。

（2）目的性，即行骗都有预期目的。否则，即使某行为是假的（比如魔术），却不具有目的性，那就不能算作欺骗；对行为对象来说，这种假动作更像误会。

（3）社会性，即欺骗是一种社会行为，产生于互动过程中：或者由一个人指向另一个人，即一个人欺骗另一个人；或者在外界影响下，同一人的人格中，某些结构的相互作用，即自欺欺人。

凡不具备这三个要素的行为，均不是欺骗。

欺骗的种类非常多。从善恶角度来分类，既有善意欺骗，也有恶意欺骗；当然，本书重点研究恶意欺骗。善意欺骗的特征是：对于个人之间来说，表现为利他，比如，大夫对绝症病情的隐瞒。对于群体间的善意欺骗来说，则表现为利己，即有利于行骗者的群体，比如，战场上的使诈。恶意欺骗的特征：对于个人之间来说，表现为利己而害他，比如，电信诈骗；对于群体间的恶意欺骗来说，表现为利己（包括利己利他、利己害他）。

从涉及欺骗各方是否为个人来看，欺骗又可分为个人之间的欺骗、双向欺骗、自我欺骗、个人与集团之间的欺骗、社会欺骗（比如邪教）等。

根据欺骗的内容，又可分为经济欺骗、政治欺骗、军事欺骗、感情欺骗、情报欺骗、舆论欺骗、新闻欺骗、信仰迷信欺骗、艺术欺骗、科技欺骗、游戏欺骗等，以及上述各种欺骗的综合。

按欺骗延续的时间来分类，又可分为瞬时欺骗、短时欺骗和长时欺骗等。

善意欺骗的正功能包括：保护功能（比如，防止亲人过度悲伤）、维持人际关系（比如，每个人都有自己的隐私）、创造功能（比如，家传秘籍）。善意欺骗的负功能，主要为“弄巧成拙”。恶意欺骗的正功能包括：破坏功能（比如，国家之间的情报欺骗）、阻抑功能（比如，行骗导致心虚，从而减损其自信度）。恶意欺骗，偶尔也会产生正功能，比如，喝到假农药，保下一条命等。

构成欺骗的必要条件包括：行骗者和受骗者的存在、特定的（或可行的）欺骗内容、必要的传递工具及传播渠道。行骗者的需要是产生欺骗的根源。受骗者的欲望常常是自己被骗的内在原因。

受骗者的心理特征主要包括：意志薄弱、过分慈善、认知缺陷（无知或错觉）、心理防御过分迟钝或过分敏感、信息匮乏、从众心理、贪心等。受骗者被选中的原因主要有三个：首先，对行骗者有利可图；其次，在众多潜在的、有利可图的备选中，受骗者的资源比较丰富，因此，欺骗的成功率就较高；最后，行骗比较“安全”，即使行骗失败后，后果也不太严重。

骗子在骗你前，常常会先营造欺骗环境，主要有以下四个要点。

（1）唤起你的信任感。其手段至少包括：用良好的声誉影响你（比如，让你身边的亲朋好友等都来称赞他），用诚实、正直的形象感化你，向你展示开朗而富有魅力的笑容、用可以信任的语调、讲述令你羡慕的个人传奇（比如，大额度的慈善捐款等），恭维奉承你，博取你的怜悯同情，当然还会针对你的个性营造特殊的情境等。

（2）装成老实人。这既是为了唤起你的信任，但也有它本身的特点，其本质在于，骗子让你觉得他很笨，从而使你放松警惕，以为在同老实人打交道，从而不再防备他的圈套。当然，此法的另一种变异就是：骗子让你觉得自己很聪明，于是便可让你“聪明反被聪明误”。

（3）利用伪证来引诱。骗子以间接的手段，提供某些信息，让你自己根据这些信息，自愿做出有利于骗子的判断。其技巧在于，提供了无可挑剔的定向事实后，你必然会据此做出自损的结论。

（4）设置“平行现实”。形象地说，就是制造相应的假象，吸引你的注意力，然后对你下手。

骗子行骗的着力点，主要体现在以下几个方面：

（1）利用生理和心理本身的若干缺陷。比如，注意力、记忆力、无条件反射、条件反射和行为规则、思维分析、疲劳、药理影响等方面的缺陷。

（2）利用逻辑与理智的缺陷。骗子利用偷换概念等手段，貌似合情合理地开展行骗活动，而普通人一时还反应不过来，无法揭露其逻辑推理中的某些漏洞。

（3）利用特殊的心理状态。这时行骗的主要着力点包括：利用受骗者的愿望、爱

情、忌妒、崇高的动机、失控的情绪、人性弱点（贪婪、愚蠢、恐惧、虚荣、怯懦、好色等）。

骗子常用的面具包括：

（1）伪善。最难识别的欺骗，是骗子把自己隐藏于友情与关爱的面具后面，以伪善形式出现。伪君子不仅作恶，有时也会行善；当然，他会隐藏自己的卑鄙动机，而假装十分高尚。

（2）背信。对骗子来说，伪善只是手段，行骗才是目的，所以只要时机成熟，他就会毫不犹豫地露出真相，背信弃义。毕竟，骗子压制本性，自己也会不愉快。

（3）无耻的谎言。在骗子的内心深处，其实也知道自己的行为不当，所以为了让自己不受良心谴责，也为了让受骗者更容易上当，他经常会编造一些谎言。

可惜，越是无耻的谎言，就越容易让人轻信。我们需要重点识破的，也是骗子常用的行骗方法主要有：

（1）暗示法，包括被动暗示法和主动暗示法。被动暗示法成功的重要因素有三点：一是施行暗示的人，对于受暗示者拥有绝对权威性；二是受暗示者有可能接受暗示；三是具体的策划必须巧妙、严谨，使受暗示者深信不疑。最典型的被动暗示法，就是众所周知的催眠术。主动暗示法，又称自我暗示法，它常见于气功中，甚至可以说，做气功的全过程都充满了自我暗示。

（2）伪装法，包括物理伪装、心理伪装和生理伪装。伪装的最终目的是给受骗者造成判断失误，包括知觉上失误（错觉）和思维判断的失误，因此，一切伪装都可归结为心理伪装。不过，物理伪装最直观，故又称为自然伪装，它利用对方的错觉，达到隐藏目的。比如，军事中常用的物理伪装有隐形伪装、象形伪装、变形伪装、听错觉伪装、嗅错觉伪装等。

（3）假面具法。这是一种典型的心理伪装，此时骗子扮演成某种角色来行骗，比如，冒充警察等。施行此法时，骗子必须具备三个条件：首先，有一定的基础，使得所扮演的角色不容易“露馅”；其次，需要有其他方面的配合，否则成功率将不高；最后，所扮角色要有一定的稳定性，否则也会失败。

（4）行为替代法。它其实是假面具法的一个特例，它仅限于角色行为扮演（比如，假冒他人去失物招领等），不包括身份、语言、地位等的扮演。此法生效的前提是，受骗方不了解被替代者的外貌特征、语言、生活及行为习惯等相关情况。

（5）现场伪造法。此法生效的关键是，伪造得自然，丝毫不显做作，骗局难于识破。伪造的隐秘性越好，对方就越容易上当。历史上，孙膑的“减灶退敌”就是此法的经典例子。

（6）销毁痕迹法。它其实是现场伪造法的一个特例，高明的网络黑客，退出你的系统后，一定会优先考虑运用此法，以避免留下作案痕迹。

（7）抵押法，即骗子以人或物作抵押，骗取对方的贵重物品。此法主要属于经济欺骗。此法的特征主要有：首先，表面看来，抵押物的价值大于待骗物，当然，实则相反；其次，以假充真；最后，有时抵押物虽然是真的，但是有其他问题，比如，用赃物作抵押等。

（8）愚弄法，即骗子利用对方的愚昧或无知来行骗。此时，骗子的常见工具包括宗教迷信和科学技术等。

（9）插脚入门法，即先小骗，再逐步升级，施行大骗。当情感欺骗时，骗子就常用此法，一点一滴地加码，最终让对方落入圈套。

（10）报酬引诱法，即给受骗者一定的报酬，达到行骗目的。这里的报酬，既可以是物质的，如实物或钱物报酬，也可以是社会及心理的，比如，赞美报酬、情感报酬，微笑报酬，以及荣誉、社会地位报酬等。

（11）长线钓鱼法，即放长线，钓大鱼。此欺骗法有三个特征：首先，骗局行设时间长；其次，隐蔽性很强；最后，骗子的目标和行为较为统一，看起来符合正常的行为逻辑。卧底间谍，就是此类骗术的代表。

（12）证章伪造法，包括伪造证件、票证和印章等。

（13）认知协调法，即行骗者努力调整被骗者的认知，使得它与欺骗行为尽可能一致，从而达到欺骗目的。比如，在自我欺骗时，“烟虫”会找出许多理由，来让自己的吸烟行为“合理化”；在诱骗他人时，传销头目会给学员洗脑，让他们觉得“拉亲属入伙”是为亲人造福。

（14）夸张法。此法可出现在几乎所有类型的欺骗行为中，夸张的内容包括：地位、身份、能力、富有程度、家庭背景、社会关系等。在运用此法时，受骗者相信事件是真的，却不知事件的范围和规模；相信某人具有某方面的能力，却不知其能力究竟有多大。任何人都希望得到“能人”的帮忙，骗子正是利用了这种心理倾向，使用夸张法来行骗。夸张法还有一种变形，称为缩小法，即把前面夸张的东西缩小；当然，目的仍然是使对方上当，比如，前面提过的“减灶退敌”。

（15）强制法。它采取强制手段，使受害者由被迫服从，到主动遵从。强制法之所以能生效，是因为强制能导致屈从，屈从可转为内化。许多屈打成招，就是此法的“杰作”。

（16）恐怖法。此法与强制法，既有相同之处（二者均含恐吓与强迫的成分），但更有差别：强制法借助武力，而恐怖法却是以后果的严重性来威胁，使受害者极度恐惧，并渴望获得解救；当骗子提出某种“良策”后，受骗者立即主动从之，并没有内化过程。从骗局的成因来看，强制法是由外力所致，而恐怖法却是由内部压力所致。恐怖法常见于迷信欺骗和科技欺骗中。

（17）信息控制法。它通过操纵信息的内容、数量等来欺骗受害者，包括信息保密欺骗法（比如，隐藏婚外情）、信息中断欺骗法（比如，新闻封锁）和信息筛选欺骗法（比

如，报喜不报忧）等。信息控制法的特点主要有三点：首先，信息操纵者有明显的功利目的。其次，经选择后传播的信息可能是真的，但让受信者误以为没别的重要信息。再次，如果未传递的信息仅是偶然事件，那受信者多半不会怀疑；相反，若未传递的信息属于常规信息，且其中部分信息已由其他渠道传播，那么公众就会产生疑虑，从而形成强大的压力，迫使新闻部门适当扩大选择信息的范围。

（18）权威作用法，即骗子冒充某方面的权威，招摇撞骗。当然，也有个别权威，依仗自己的影响来行骗。

（19）调虎离山法，由《三十六计》中的调虎离山计演化而来。

（20）谣言法。此法很特殊，将在随后详细介绍。

（21）综合性骗术，即将各种欺骗方法巧妙结合起来，达到行骗目的。

总之，骗子必定要为所谓的“真相”营造一个虚假模式，并试图操控受骗者按骗子的意愿行事。骗子最主要的操控方法包括信息操控和意识操控等。

信息操控的常见方法有隐瞒、选配、作假、曲解、颠倒等，下面进行具体介绍。

（1）隐瞒。这是最简单的欺骗，即向受骗者隐瞒真实信息。此时，受骗方已对某一现象或事件有了不正确的概念，而行骗方并未告知真相。表面上看这里没谎言，结果却引起受骗方的误解。

（2）选配，即只把部分有利于骗子的（真实）信息灌输给受骗方，而不说另一部分不利于骗子的信息。这就可能让受骗者形成曲解事实的虚假概念。

（3）作假，也叫弄虚作假，即提供虚假信息，意在突出和强调一些有利于骗子的现象。

（4）曲解，包括夸大或缩小。具体地说，骗子将有利于自己的论据强化，将有利于对方的论据弱化，从而达到操控受骗者意识的目的。

（5）颠倒，比如，是非颠倒、黑白颠倒、有无颠倒、真假颠倒等。

当然，还包括上述五种骗术的各种组合。

意识操控，就是骗子设计一套步骤，引诱或逼迫受骗者，自愿做出有利于骗子的行为，而受骗者还误以为这些行为对自己有利。最常见的意识操控就是所谓的激将法。当骗子设计骗局操控你的行为时，最有效的办法就是换位思考，即以你的角度来判断：在何种情况下，会做什么动作。

第 2 节　伪装的基本原则

学习提示

- 掌握良好伪装的九大基本原则和四个重要特性。
- 掌握在充分调研的基础上确定了伪装对象后，如何提升伪装的真实性，如何将个人

爱好巧妙植入交流过程，如何把握好伪装力度，如何学会使用对方的语言，如何避免不必要的信息泄露，如何尽量简化伪装，如何处理好后事等。

案例导入

社工攻击的核心是欺骗，欺骗的关键之一是伪装。在一般性地讨论伪装之前，先做一个实验：如果要求你在白天进入一个保安措施齐全的大楼，你将会怎么办呢？你肯定不敢撬锁，也不敢翻墙或跳窗，更不敢靠武力硬闯。虽不知到底如何才能万无一失地进入该大楼，但至少应先进行适当的伪装，比如，外貌打扮必须尽可能像是楼内的办公人员，否则一进大厅就会被保安盯住，更甭想混入楼内。事先你得对大楼的结构有所了解，至少该知道出入口在哪里，总不能在大厅里像无头苍蝇那样乱撞，否则就会被保安毫不客气地赶走。事先得搞清楚入门的条件，若需通行证，你得弄一个尽量逼真的证件；若能混迹于人群，你得在高峰时期开始行动；若能尾随其他访客，你也得先混迹于某个真实的访客群体；若进楼时必须输入某个密码，你就得先想办法弄到出入门的密码。如果实在不能获得入门的证件或密码，你也可以随时紧盯门卫，万一他在某个时刻稍有疏忽，你就可以趁机溜入。当然，为了尽可能不暴露自己的行踪，避免引起不必要的注意或不被事后溯源，你还得事先摸清大厅的监控体系，尽量待在摄像头的视线之外。

总之，伪装工作非常困难，需要考虑的因素实在太多，很难不出现疏漏。作为一名合格的社工人员，必须拥有强大的心理承受能力，至少在出现疏漏时能够镇定自若地随机应变，化险为夷。

与上节的欺骗类似，伪装在许多情况下都被当成贬义词。不过，从纯学术角度看，我们宁愿将伪装理解为中性词，即伪装被定义为以他人的身份来表现自己，基于新的背景故事、衣着、外表、个性和态度等来塑造新角色，从而达到既定目的（比如，获得他人的隐私信息等）的行为。在某些情况下，社工黑客需要伪装一个全新的身份，然后利用该身份来从事一些特殊活动。如果新身份越陌生，伪装的难度就越大。伪装得越全面就越令人信服，伪装得越简单就越容易成功，露馅的可能性就越小。伪装是社工攻击中难度最大的工作，没有任何一种伪装是万能的，每一种伪装都必须量身定制。不过，关于角色扮演式伪装，还是存在着一些普适性的基本原则。简单来说，良好的伪装必须具备四性：一是积极性，即伪装的目的必须符合既定意图，不仅要采取隐真措施，还要积极示假。二是自然性，即伪装要符合实际情况，力求逼真。该隐蔽时，要符合自然背景；该变化时，要与实际情况相适应；该示假时，假目标要尽量逼真。三是多样性，即伪装措施要灵活多样，不能千篇一律。四是连续性，即伪装过程要及时而不间断地进行，起止时刻最容易露马脚。具体来说，伪装有下面九大原则。

原则一，事前的调查越充分，伪装成功的可能性就越大。前面已经多次强调，社工攻击（当然也包括伪装）成功的关键是事前的充分调查和信息收集。事前的信息收集得越广