有点疑惑？举个例子分析一下。如果要得到某个绝密产品的化学成分，你要诱导的目标是制造该产品的一位化学家，并且决定和他谈论化学，那么此时你不能伪装成一个世界级的化学家（除非你真是）。他可能在交谈中提出一些你一无所知的问题，那样你就演砸了，诱导行动也就归于失败了。

更加现实的方式是伪装成一个学习某专业的学生，得知他在这个领域有惊人的造诣。基于他的专业知识，你只是要问他一个与自己正在研究的化学分子式有关的问题，问他该分子式为何没有效果。

重点是，不管你选择谈论哪个话题，也不管你选择和谁交谈，都要做些研究、反复练习且精心准备。一定要具备足够的知识，就目标对象会感兴趣的话题侃侃而谈。

(3) 切忌贪婪。当然，诱导的目的是获取信息、得到答案或者取得进入某领域的钥匙。然而，不要将此作为重点。如果你一心想得到自己需要的信息，很快就会被目标看穿，导致目标失去兴趣。通常情况下，给对方一些感兴趣的东西会引起对方的交换情结（第6章会讨论），这样对方会觉得有义务给你一些回报。在交谈中这一点很重要。交谈中要有来有往，除非对方是一个滔滔不绝的人。如果他谈论不止，就让他说。如果你得到了一些信息，就适可而止，不要贪婪地不断深挖，否则会引起对方的警觉。

有时，世界上的“最佳交流者”其实是那些听的比说的多的人。

这3个成功诱导的步骤能有效改变你和其他人在日常生活中的交流方式，不仅对社会工程人员和安全审计人员有益，对普通人也是如此。我个人想在这“3个步骤”上再加1~2步。

例如，交谈中诱导的一个重要方面是面部表情。表现得太紧张或太放松都会影响人们对你问题的反馈。如果你言辞镇定，并且吸引了目标参与交谈，但是身体语言或面部表情却表现得漠不关心，这会影响对方的情绪，即使他自己并没有意识到这一点。

下面这个例子可能稍显突兀，但我是塞萨尔·米兰（Cesar Milan，也称“狗语者”）的粉丝。我认为他是个天才。他可以与那些难以驯服的狗沟通。仅仅只需要几分钟时间，他就能让狗和其主人产生一种特质，从而让他们形成亲密的关系。他主要是教授人们怎样与狗沟通，即怎样通过狗可以理解的语言要求或告诉狗去做某事。他的理论中有一点我很认同，就是人的“精神”或活力会影响狗的精神或活力。换句话说，如果一个人走近狗的时候处于精神紧张且焦虑的状态，那么即使他的言辞显得很镇定，狗也会紧张、狂吠甚至具有攻击性。

显然，人和狗是不同的，但我认为上述理论同样适用于人。当社会工程人员接近目标时，他的精神或活力会影响对方的感知。活力会通过肢体语言、面部表情、穿着打扮等各方面表现出来，语言只是一种辅助的表现方式。在不知不觉的情况下，人们就会有所感知。你有没有想过或者听别人说过，“那家伙似乎很猥琐”或者“这姑娘看上去很友善”？

这背后的原因是什么？一个人的精神或活力会传递到你的“感知器”，这些数据会和以往的经历相关联，从而形成一个判断。判断会立刻形成，很多时候连自己都不知道。所以在进行诱导工作之前，必须使你的活力与所扮演的角色相匹配。如果你的个性或精神特质不能使你轻易伪装成一位经理，那么就不要尝试去这么做。必须找到适合你的角色和切入点。就我个人来说，我只是一个普通人，强项不在化学或高等数学上。如果要参与化学和高等数学方面的对话，我不会扮演一个对二者十分精通的人，而是会伪装成一个只想随便聊聊天气的陌生人。

不管你选择使用何种方法，都需要做一些准备工作，以期得到更好的结果。其中的一个步骤可以称为铺垫。

3.2.1　铺垫

排队买10美元一张的电影票时，会看到很多即将上映的影片的海报。等到你排队买40美元的爆米花和饮料时，会看到更多的海报，然后一路挤到自己的座位上。最后，电影正式开始前，还会放映一系列影片的预告片。有时，有些影片还没有开始制作，广告和预告片却已经到处都是，广告中可能会说“这是自……以来最有趣的影片”，或者随着一段恐怖的音乐响起，屏幕上烟雾弥漫，画外音提示“你认为‘少年杀手第45部’已经结束了……”，极尽精彩之处。

不管是什么电影，营销攻势都会告诉你如何去感受电影，换句话说，也就是在试映之前通过铺垫植入你应该对电影产生的看法。通过两三分钟的预告短片显示影片的概貌，让你产生看这部电影的意愿，并且呼吁那些想看喜剧片、恐怖片或爱情片的人前去观看。

虽然之前关于铺垫的文章不多，但这是一个严肃的课题。铺垫意指你可以按照它说的做——通过植入的信息或观点影响目标对特定信息的反应。铺垫常用于营销信息中，例如一些全国性连锁餐馆会通过广告展现人们微笑着享用美食，食物看起来精致而完美。当画面中的人说“太好吃了！”或者“哇噢！”的时候，你似乎也能感觉到其中的美味。

当然，社会工程人员不能通过商业广告来影响目标，那么如何在社会工程过程中应用铺垫技术呢？

在大多数社会工程应用中，你得从最终结果出发，确定开始时应该做哪些准备工作。你的目的是什么？你诱导的一般目的可能是获取对象工作项目的信息，或者他在办公室/度假的时间。不管是什么，必须首先设定目标。接下来要决定你要问何种类型的问题，然后才能决定如何植入一些前期信息，诱使对方给出你想要的答案。

例如，晚上你想要去某个地方吃牛排，但是喜欢使用折扣券的妻子并不喜欢那家餐馆，而你却时时刻刻想着那些肋眼牛排，此时就可以通过意念植入来影响对方。早晨你可以无意中说起：“亲爱的，你知道我在想什么吗？一块大大的、鲜嫩多汁的烤牛排。前几天我开车去邮局，看到邻居弗雷德将烧烤架放在路边，用木炭烤牛排，香气从车窗飘进来，从那以后我就一直想吃牛排。”

这个时候，妻子对这个诱导有没有反应并不重要，你已成功植入了一个思想的种子。她会设想牛排在烤架上滋滋作响，然后你接着说烤牛排的过程，说弥漫的香气，说自己有多么想大快朵颐。

如果接着你带了份报纸回家，浏览中发现有目标餐厅的广告，上面有折扣券。只要将折扣券页面折叠放在桌上即可。当然，你的妻子可能看到，也可能没看到。但是，因为你把它和信件放在了一起，之前提到了牛排，而且她喜欢折扣券，所以桌上的折扣券会引起她的注意。

过一会儿，她可能会过来问你："今晚想吃什么？"这就是你之前一系列铺垫工作所发挥的作用——你提到了飘香四溢、鲜嫩多汁的牛排及自己的渴求，你将目标餐厅的折扣券放在桌子显眼的位置上，现在是晚餐讨论时间。你可能会回答："今晚如果在家里吃的话，你不仅得做饭还得花时间清理，我们已经有段时间没去XYZ牛排馆了，今晚我们去那里如何？"

因为你知道她不喜欢那个餐馆，所以希望之前的铺垫工作能发挥作用。她回答道："我看到报纸上有那个餐厅的折扣券，第二份半价，但是你知道我不喜欢……"

在她说的时候，你可以用赞赏的语气插话："哈！折扣女王再次出击。我知道你不大喜欢牛排，但是我听莎莉说那边的鸡肉也很棒。"

几分钟之后你就会在去那个餐厅的路上。如果没有前期准备工作，你很可能会得到干脆的拒绝："不去。"铺垫工作对她的思维产生了影响，使她接受了你传递的内容并最终发挥了作用。

再看另外一个非常简单的例子。一个朋友走过来说道："我告诉你一件特别有趣的事情。"你会怎么反应呢？可能在他说出之前你就开始微笑了，你期待一个好玩的故事，所以在等待一个大笑的契机。他对你进行了铺垫，使你对幽默故事无限期待。

在社会工程领域如何应用这些原理呢？

铺垫本身就是一种技巧。以一种隐晦或婉转的方式植入想法或思路，比诱导本身更需要技巧。根据目标的不同，铺垫有时是相当复杂的。前面牛排的场景就是一个复杂的问题。铺垫需要投入时间和精力，特别简单的铺垫可能就是找出对象开的是哪个品牌的车或者其他一些看似无关紧要的信息。你可能"碰巧"与目标处于同一家熟食店，于是开始一次随意的聊天，你说道："哥们，我很喜欢自己的丰田车。刚刚在停车场有个开雪佛兰的家伙倒车时撞了我的车，结果连个划痕都没有留下。"如果足够幸运的话，你对丰田车的评论会引起对方的兴趣，随后你们可能会讨论车型或你想了解的其他话题。

在开始分析如何利用诱导的同时，考虑铺垫的问题会更有意义。社会工程人员从一开始就掌握了这一技巧。很多时候，社会工程人员在开始社会工程生涯之前就已经意识到自己有该项技能了。他们在青少年时期就发现与人沟通很简单，并且随后会倾向于与人沟通的工作。也许他是所在朋友圈的中心，人们遇到问题时会找他倾诉，会和他谈论任何问题。他后来意识到这些交流技巧能让他得到很多别人不能获得的机会。

我年轻时就具有这一天赋。父母经常说起，我在五六岁时就能和完全陌生的人交流，有时我会走进繁忙的餐厅厨房，询问我们订单的情况或者菜是怎么做的。不管怎样，我做到了这一点，为什么呢？也许是因为我根本不知道这种行为的怪异，因为我非常自信。在我长大后，这种天赋（或者无畏精神）得到了更全面的发挥。

似乎人们（有时甚至是完全陌生的人）喜欢向我倾诉他们遇到的难处，喜欢和我交流。十七八岁时发生的一个故事可以说明我在利用铺垫以及诱导技术方面的技巧。

我曾经非常热衷于冲浪，所以经常会做一些奇怪的工作以支撑这一爱好，从比萨快递员、玻璃纤维切割师到救生员等不一而足。有一阵，我给父亲的财务咨询公司做些杂事，经常递送文件给他的客户，待客户签好名后再拿回来。很多客户会和我聊起来，聊他们的生活、离婚以及生意上的起起落落。通常，开始时他们仅仅是告诉我，我父亲对他们来说是如何重要。当时我很难理解，为何人们，尤其是成年人，会向一个十七八岁的年轻人敞开心扉，讲述其生活的艰辛。

有一个我经常拜访的特别的客户，他拥有一整幢复式公寓，不大也不豪华，他只是拥有并管理着这些资产。这个可怜的家伙问题真多：家庭问题、健康问题及个人问题。每次只要我一坐下来他就开始反复不停地说。从那时起我就发现，只要坐在那里听就可以了，同时我可以神游于物外或者做一些奇妙的事情。这让他们感觉自己很重要，也显得我是一个乐于倾听的好人。我完全可以坐在那里遐想下一次美妙的冲浪，关键是我给他的感觉是在倾听。

通常我会一直听，直到受不了他所喷出的“浓烟”（他抽烟比我所见到的任何人都要多）。因为我还年轻，没有经验，所以无法提出什么建议，也没有什么解决方法，只有耳朵。关键是我真的关心，并未假装，我真心希望能有一个解决方法。有一天他告诉我，他很想回到西部，他的女儿在那里，他可以离家人更近一些。

我当时正想有些变化，换个更酷且更有趣的工作，挣更多的钱，以便买更好的冲浪板和其他“需要”的东西。在一次倾听过程中，我突然冒出一个疯狂的想法，而且他也认为我是一个有责任心、有激情而且还有些头脑的年轻人。前几个月的促膝交流和倾听建立了良好的铺垫基础，现在是收获的好时机。我说：“你回去吧，这边的物业由我帮你打理如何？”这个主意很荒谬，现在回过头来看，我会嘲笑这个古怪的想法。但是我和他交流的时间加起来有好几周，甚至有几个月了，我一直在倾听他的问题，我了解他以及他的痛楚。此外，我从没有过类似嘲笑或贬低他的做法。现在，他和我分享自己的问题，而我提供了一个对他来说可能很完美的解决方案，我们可实现双赢。我在收入方面的要求不高，他也想离家人更近一些。我们通过前面几个月的沟通建立了良好的关系，他也“了解”并信任我。

经过一番讨论之后我们达成了共识，他起身回到西部，而17岁的我作为二房东帮他管理30套复式公寓。我还可以继续唠叨这个故事的细节，但我想重点已经充分表达了。（这个工作很棒，直到后来他要我帮他把物业卖掉。我及时完成了这最后的任务，这份工作也就告一段落。）

重点是我在没有任何恶意的情况下，构建了与他人的良好信任关系。我用几个月的时间与他沟通，在他的意识里构建了善良、有激情并且聪明的形象。在时机来临的时候，虽然想法荒谬，但是前期的铺垫使得这一想法能够被接受。

在重新回顾这段往事时，我有了新的认识。我当时并没有意识到这件事情当中的很多促成因素。从社会工程的角度看，铺垫工作包括在开始之前知道自己的目标。这个案例中，我并不知道最终会得到这一近似疯狂的工作，但是铺垫工作仍然起到了作用。

大部分社会工程案例的进程会更快，但我认为原则是相同的。即使是天才也必须遵守类似的原则。因为铺垫工作涉及个人的情感和意识，所以不要给他们怀疑的理由。所提的问题必须与你伪装的角色相匹配。要想准备工作奏效，之后提出的问题要与你前期植入的意识相匹配。例如，如果我的建议是到客户的家乡并给他带回一些拍摄的相片，而不是为他管理物业，就和他对我的认识不相匹配，因为我的形象是一个灵活、有生意头脑及有爱心的年轻人。最后，在目标达成时，必须对客户有益，至少让他认为有益。在我的例子中，客户能够感觉到的好处是充分的。但是在社会工程中，可能只是一些“吹嘘”，为他人提供一个夸口的平台，或者提供一些更加实在的好处，包括身体、金钱或者心理上的好处。

练习诱导，不断变得熟练，你就会变成杰出的社会工程人员。从逻辑上来讲，下一节将介绍怎样成为一个成功的诱导者。

3.2.2 成为成功的诱导者

通过分析我个人的经历，我可以总结出自己从5岁起直到现在取得成功的关键要素。

- 不惧与他人交谈，并处于非“常规”场景中。
- 真心关心他人，即使是陌生人。乐于并享受倾听。
- 只在有了真正的解决方案时才提供建议或帮助。
- 在他人说出自己的问题时，不做主观判断。

确实存在成功诱导的关键元素。美国国土安全部有一个供内部员工使用的有关诱导的小册子，我有幸拿到并放在了www.social-engineer.org/wiki/archives/BlogPosts/ocso-elicitation-brochure.pdf上。

这本小册子中有一些十分精彩的观点。基本上，按照小册子及本章中的描述，诱导的应用在于其有效性、很难察觉及不具威胁性。该手册采用了“怎样避免”的角度来描述诱导，但是其后续章节给定了一些场景以展示其要点。

1. 唤醒他人的自我

美国国土安全部的手册中的场景如下。

攻击者：“你的工作一定很重要，某某认为你很厉害。”

目标："谢谢，谬赞了，但是我的工作并不那么重要，也就是……"

唤醒他人自我的方式简单有效，但是要注意如果滥用这一强大的工具，或者不是出自真心，则会让目标失去热情。你不会到处和人说："哇噢，你真是全球最重要的人，长得还那么帅。"这样说只会引起别人的警觉。

唤醒他人的自我需要微妙的处理。如果你碰到的是一个真正的自我陶醉者，在听他夸耀过往成就时，眼珠不要转，不要叹气，也不要争论。微妙的自我唤醒要像这样，"你的那个研究改变了很多人在……方面的观点"或者"我无意中听到史密斯先生在那边说，你是他最敏锐的数据分析师"。要达到目的，但不能说得太明显。

据美国国土安全部的手册介绍，精心的吹捧会促使他人说出一些从未透露过的信息，而这正是社会工程人员想要的结果。

2. 表达共同的兴趣

考虑如下的模拟场景。

攻击者："哇噢，你有ISO 9001规范数据库的背景？那么你该看看我们开发的辅助认证的报告引擎模型，我可以发给你一个副本。"

目标："太好了。我们正琢磨着在系统中添加一个报告引擎呢。"

表达共同兴趣是诱导的一个重要方面。在上面的特殊情境里，甚至比"唤醒自我"更加有效，因为它迅速拓展了关系，超越了初始交流范畴。目标同意进一步接触，同意接收攻击者发送的软件，且表达了以后继续讨论公司软件计划的兴趣。所有这些都会导致大规模安全入侵。

此时的危险在于攻击者完全掌控了形势。他控制了下面的步骤，发送什么信息、多少信息以及何时发送。对社会工程人员来说，这一步相当有利。当然，如果是长期目标，可以找一个能共享的软件，那就更有利了。共享有用的、非恶意软件能够构建信任及和谐的关系，使目标产生进一步交流的责任感。

3. 故意说错

不经意间说错一些事情似乎会适得其反，但处理得好的话却是一件利器。

攻击者："所有人都知道XYZ公司这方面的软件销售得最多。"

目标："事实可不是这样。我们公司从1998年就开始销售类似的产品，通常我们的销售记录超过他们23%以上。"

有效使用这种表达方式会诱导目标说出真实的数据。大部人在听到错误表述时会有校正的欲望，似乎他们的正确性受到了挑战。告诉他人、显示自己的博闻强识、不能容忍错误表达等欲望

似乎是人类的天性。充分理解这一点，可以让这一场景变得很强大。你可以通过这种方式让目标说出事实的全部细节，也能在一群人中立刻发现谁对这一主题最为了解。

4. 主动提供信息

美国国土安全部的手册中对人的共性做了很好的概括。本书前面提到了一些，后面会有更详细的介绍，其中责任感就是一种很强大的力量。作为社会工程人员，在交流中主动提供信息会迫使目标提供具有同样价值的信息。

想要试一下吗？下次在和朋友聊天时这样说："听说露丝的事了吗？我听说她被辞退了，而且现在找工作也很困难。"

大部分时候你得到的反馈是："啊！没听说呢。真不幸。我听说乔在办离婚，好像房子也保不住了。"

人类具有同情心，倾向于"同病相怜"，该示例就把这一点体现得淋漓尽致。人们喜欢分享类似的新闻。社会工程人员可以利用这一倾向，为谈话设定基调或氛围，从而构建出责任感。

5. 假装高深

另一个强大的操纵工具就是假装高深。一般情况下，如果对方具有某一方面的知识，和他讨论相关问题并无不当。攻击者可以审慎地利用这一点，首先展示一些信息，假装知道一些内情，然后使用诱导技术展开话题。过程中可以把别人的观点当成自己的说出来，进一步强化自己的专家假象。下面的例子可以很好地说明这一点。

有一次，我要到A国商谈一笔大宗原材料交易。会谈需要我对目标公司具有详细的了解，而且必须要在见到他们之前做到这一点。之前我们从没见过，所以在谈判之前我去参加了一个在A国举办的会议。会议中我恰好听到了一个对话，讨论的是在和A国人的谈判中如何占上风。

我知道这是一次机会，而且更妙的是谈话小组中的一个人正是来自我要会面的公司。我快速加入其中，并且知道如果我不能快速地表达观点就会显得很尴尬。我这方面的知识不足，但是不必让他们知道。在他们谈话的间隙，我开始谈论"关系"理论。关系就是两个人（可能来自不同的社会阶层）如何产生联系，之后一人迫于压力为另一个人提供帮助。我谈到了怎样使用这种联系，总结中还提到：作为一个美国人，不能仅将名片塞进裤子后面的口袋里，而应该仔细研究、添加备注并将它们放在恰当的地方。

这番发言足以显示我的学问，让我有资格被列入值得信赖的人之列。表达过自己的观点后，我坐下来听其他人讲述自己的经验以及他们和A国大公司谈判方面的个人心得。目标公司的那位先生开始发言时，我更是极度关注。我敢肯定他发言中所表达的"观点"与其公司的经营理念紧密相关。这项收获比我能买到的信息都要有价值得多，也使得我后来的A国之行得以圆满成功。

还有一些诱导中常用的场景。

6. 利用酒精的影响

在挖掘秘密方面没有比酒精更有效的东西，这一点很悲哀，但却是事实。如果在上述5个场景中加入酒精元素，则效果会放大10倍。

也许最好的方式就是以真实的故事来阐明。

1980年，洛斯阿拉莫斯实验室的一位资深科学家访问B国的一个研究院，举办一个关于他的专业——核聚变的讲座。他在核武器方面具有丰富的知识，但他知道这方面是禁区，所以需要将讲座的内容限定于他的研究主题。

过程中，有很多问题与核武器直接相关，且问得越来越细。攻击者的战术也会改变，他们也会问一些有关聚变和天体物理方面的问题。

在为他庆祝的鸡尾酒会上，人们不断走上前，赞扬他的学识和研究，每次都要祝酒和干杯。逐渐地，人们开始问一些绝密问题，例如氘和氚的点火要求，这两种元素都是中子弹的组成部分。他对这些问题防护得很好，但是在喝多了之后，他决定给出一个类比。他于是说，如果将这两种元素混合成一个球从桌子上滚下来，它们就可能点燃，因为它们的燃点都很低。

这个看似无用的信息可能为B国的核武器研究者提供了清晰的指引。他们会与另一位科学家交流，然后得到更多的知识，以此类推，逐渐获得越来越多的知识。在很多尝试之后，B国的科学家终于掌握了清晰的蓝图。

这是一个利用诱导术逐步获取整个答案的真实案例。你也可以在社会工程活动中采用诱导术。所有的答案并非来自同一个地方。你可能从某人口中得知有关日期和地点的信息，然后使用这一信息从他人口中诱导出更多的信息，以此不断深入，直到得到全部的信息。如何将这些信息聚合在一起，这是其中最困难的部分，需要完美的诱导技巧，这会在后面讨论。

3.2.3　提问的学问

作为社会工程人员，你必须认识到，诱导的目的不是走过去问："你们服务器的密码是什么？"

你的目的是得到一些看似无用的琐碎信息，然后使用它们构建出你所寻求的答案的全貌，或者通过它们一步步取得答案。不管使用何种方式，这类信息收集方式都会为社交人员达成目标指明清晰的方向。

如何知道使用何种类型的问题？

下面将分析存在的几类问题以及社会工程人员如何使用它们。

1. 开放式问题

开放式问题不能仅仅用"是"或"否"来回答。如果是问"今天外面相当冷啊，是吧？"，

得到的只能是“是啊”、“啊”、“嗯”之类的答案。如果你的问题是“你觉得今天的天气如何？”，那么引出的就是有效的回应，而不仅仅是“是”或“否”。

社会工程人员可以通过分析和研究优秀的记者来学习如何使用开放式问题。优秀的记者必须使用开放式问题，以持续诱导被采访对象回答设定的问题。

设想我约了朋友会面，但是他取消了这次活动，我想知道具体原因。我的问题会是这样的：“你取消了前几天的会面计划。到底是怎么回事啊？”

“我感觉不太舒服。”

“哦，希望你现在好点了。什么地方不舒服？”

通过这一连串的问题通常会得到更多的信息。如果仅仅是责备的话，效果就不一定了，比如问道：“伙计，到底是咋回事啊？那天你竟然放我鸽子！”

开放式问题的另一个强大之处是多使用为什么和怎样。如果问题中包含为什么或者怎样，就会得到对原始问题的深入解释。

这些问题都不是通过“是”或“否”就能回答清楚的，对方会暴露一些你感兴趣的细节。

有些人会抵触开放式问题，所以使用金字塔方法会好一些。先从范围较窄的问题开始询问，随着谈话的进行会聊到更宽泛的问题。如果你真想用好这一技术，可以从询问青少年开始训练。

例如，很多时候开放式问题会是这样的：“今天上学怎么样啊？”得到的回答会是：“还行。”再无他言。这样的回答没有任何意义，所以问一些范围较窄的问题会得到更多的信息。

“今年你们数学教什么？”这个问题的范围很窄，只能用特定的回答：“代数II。”

“啊，我很讨厌代数。你喜欢吗？”

从这里开始，可以拓展到更宽泛的问题，而且一旦使目标打开了话匣子，获取信息就变得容易多了。

2. 封闭式问题

显然，封闭式问题正好和开放式问题相反，但也是一种有效引导目标的方式。封闭式问题经常会限制回答的范围，通过不超过两种可能。

使用开放式提问，问题可能是：“你和经理的关系如何？”但封闭式问题就会是：“你和经理的关系好吗？”

封闭式问题的目的通常不会是要得到详细信息，而是要对目标进行引导。

司法人员和律师经常运用这种类型的推理。如果想要目标遵循特定的回答路径，他们的问题经常是封闭式的，不允许答案出现天马行空的可能。常见的询问方式如下。

“你认识被告史密斯先生吗？”

“是的，我认识。”

“6月14日夜晚，你在ABC酒店看到史密斯先生了吗？”

“看到了。”

“当时是什么时间？”

“晚上11点45分。”

所有这些问题都是封闭式的，应答只有一到两种可能。

3. 引导性问题

引导性问题结合了开放式问题和封闭式问题的特性，是具有答案暗示的开放式问题。例如，“6月14日晚上11点45分左右，你和史密斯先生在一起在ABC酒店，是吗？”。这种类型的问题会引导对方，并且为其提供表达自己观点的机会，但是其发挥的空间很狭窄。同时引导性问题暗示目标你对问题的答案已经有所了解。

引导性问题的答案经常为“是”或“否”，但是与封闭式问题有所不同，因为问题中植入了更多的信息，所以社会工程人员也能从中得到更多的信息。引导性问题陈述了部分事实，然后询问目标是否同意。

1932年，英国心理学家弗雷德里克·巴特莱特（Frederic C. Bartlett）总结了记忆重构的研究结果。他告诉实验对象一个故事，然后让他们立即回忆其中的事实，两周以后以及四周以后再次进行回忆。巴特莱特发现，实验对象根据他们的文化背景、信仰和个性修改了故事，没有人可以正确地回忆出完整的故事。这证明了记忆并非是对过去的正确记录。似乎人们会构造记忆来契合自己对世界的已有认知。在被询问时，很多情况下，我们的记忆库是基于自己的感知和对自己重要的事情而形成的。

正是因为这样，通过引导性问题来操纵人们的记忆是可行的。伊丽莎白·洛夫特斯（Elizabeth Loftus）是一位目击者证词研究领域的开拓者，她演示了通过使用引导性问题扭曲人们对某事的记忆是极有可能的。例如，如果你给他人看一张没有放泰迪熊的孩子房间的照片，然后问他：“你有没有看到一个泰迪熊？”你并没有暗示他房间里有一个泰迪熊，所以他会按照自己的想法回答“有”或“没有”。然而，如果问题是“你看到泰迪熊了吗？”，这就暗示了房间中有泰迪熊，通常人们的答案会是“看到了”，因为泰迪熊与人们对孩子房间的认识具有相关性。

这些研究表明，引导性问题是专业社会工程人员手中的一件利器。学习怎样引导目标也会增强社会工程人员收集信息的能力。

4. 假设性问题

假设性问题就是其字面的含义——你会假设对象已经拥有特定的知识。通过假设性问题，社会工程人员能够确定目标是否拥有他想要的信息。

例如，司法人员采用的一门技巧就是假设目标了解某些事（如了解某人），于是会问："史密斯先生住在哪里？"根据问题的答案，该司法人员可以确定目标是否认识对方及其熟悉程度。

社会工程人员在使用假设性问题时，有一点需要注意，即不要让目标了解事情的全貌。如果目标了解了整个意图，社会工程人员会丧失对环境的部分控制能力，控制权会反转。社会工程人员也不能通过假设性问题指责目标的失误，这样会疏远目标，同样导致自己丧失控制权。

在使用假设性问题时，社会工程人员最好已经对事实有所了解，然后将事实贯穿在问题中。如果假设性问题中携带了虚假信息，只会让目标失去兴趣，得到的结果只能是目标不知道某些不曾发生的事情。回到前面的例子，为了从一位重要的化学专家那里获取信息，我做了一些前期研究并学到了足够的知识，也许可以问出一个精妙的假设性问题，但是如果我不能满足目标对我知识的预期，则会将整件事搞砸。

举个例子，假设我的问题是："因为氘和氚的温度阈值都很低，在处理它们的时候怎样避免燃烧呢？"如果我不是核物理学家，可能很难理解后续的内容，这样会适得其反而且没什么用处。要对假设性问题进行规划才能取得最大的效果。

在询问假设性问题时，司法人员掌握的一件有用的法宝就是："在回答下一个问题之前，请考虑清楚……"这句话给对方的暗示就是在回答问题时一定要诚实。

掌握这些技巧需要成年累月的训练。如果前几次尝试不成功也不要沮丧，要不断尝试。不要有畏惧，下面有掌握这一技巧的窍门。最后还会有一个综述。

3.3 精通诱导

本章有很多信息需要消化吸收，如果你不是那种善于和人打交道的人，使用本章的技术会很艰难。与社交工程的大多数要素一样，诱导在应用中有一系列的原则，能够强化个人的沟通技巧。为帮助你掌握这些原则，请记住以下几点。

- 问题太多会吓跑目标。用一堆问题轰炸目标不会有任何收获，只会让对方害怕。记住，对

话是一种有来有往的交互，你想要问，但也要告诉对方一些信息，让对方感到自然。

- 问题太少会让对方不自在。你曾经碰到过“尴尬沉默”的场景吗？这样不会有效果，对吧？不要假设目标善于交谈，会长篇大论、滔滔不绝。你必须研究谈论的问题，让对话有趣。
- 一次只问一个问题。第5章会涉及思维缓冲区溢出，但是在这里你的目的不是使对方溢出，而只是收集信息，构建答案的轮廓。不能显得太急切，也不能兴味索然。

根据已收集的信息，要使诱导正常发挥作用需要微妙的平衡。信息太多、太少、太急切及不充分都会导致失败。

不过，这些原则有助于你掌握这一惊人的才能。不管是将该方法用于社交工程中，还是用于学习社会交往的技巧，都应遵循如下方法：将谈话想象成一个漏斗，上面是最大的、最“中性”的部分，底部是最窄的、最直接的部分。

开始时问一些相对中性的问题，通过这些问题收集一些情报。在对话中要你来我往，然后问一些开放式问题。如有需要，使用几个封闭式问题引导目标到我们感兴趣的部分。如果情况允许，进入漏斗底部，询问那些最直接的问题。从这个漏斗中流出的就是源源不断的有价值的信息。

考虑前面讨论的商业聚会酒吧中的情况，我的目标是获取情报，然后发起一次安全入侵。

交谈开始时我的问题是很中性的。“想清静片刻？”这个问题打破了对话的坚冰，通过其中的幽默元素为双方建立了平等沟通的桥梁。我又问了几个中性的问题，在问他的工作时呈上了自己的名片，这样对话持续平稳地进入了开放式问题环节。

经过前面简短的信息收集环节，可见谨慎地使用预设的封闭式或假设性问题是关键。当得知公司最近购买了新的财务软件且网络也升级了之后，我需要的就是以此为切入点且完成任务。通过对大楼安全措施的了解，我知道使用的是RFID，但不是很确定目标会进一步说明门卡的样式，并拿给我看。

这里就要应用直接的问题，即明确地询问公司使用的安全方式。在我使用这类问题时，我们的关系和信任程度已经达到很高的级别，他可能回答我提出的任何问题。

懂得如何与他人沟通是诱导者必须具备的技巧。社会工程人员必须适应并且能融入任何环境及情况下的交流。迅速建立与目标的初步信任是关键步骤，没有友好的关系，交流极有可能以失败告终。

其他的重要因素包括确保你使用的沟通形式、询问的问题以及说话的方式与自身的伪装相匹配。虽然知晓如何问出一个目标必须回答的问题是成功诱导的关键，但是如果所有的技巧和问题与你的伪装不匹配，则诱导也会失败。

3.4 小结

本章涵盖了全书最强有力的一些观点。之所以说“强有力”，是因为诱导技巧不仅会提升社会工程能力，也能提高沟通的水平。明白如何通过正确的节奏和方式问出恰当的问题，可以得到很多机会。作为社会工程人员，这是成败的分水岭。第一印象往往取决于外表，但是从你嘴里说出的话更是成败的关键。精通诱导技巧几乎可确保社会工程人员的成功，也会为你所扮演的角色大大加分。

本章也提到了伪装的强大之处。这是每个社会工程人员都需要关注的另一课题，无论是恶意的社会工程人员，还是专业的社会工程人员，都必须掌握。但是怎样确保实现这一目标呢？要回答这个问题，必须学习和理解何为伪装，详见第4章。

第4章
伪装：如何成为任何人

诚信是建立关系的关键。如果善于伪装，也能成功。
——理查德·杰尼（Richard Jeni）

有时我们会希望自己变身为另外一个人。我就常常很见鬼地希望自己能稍微瘦一点，帅一点。即使医学界还没有研发出一种快速变身的药物，但是解决这种窘境的方法确实存在，那就是伪装。

什么是伪装？有的人认为只是社会工程过程中编造的故事或者谎言，但是该定义是非常狭义的。更为精确的定义是，以背景故事、衣着、仪表、个性和态度来塑造角色以完成社会工程审计工作。伪装包括你所能想到的基于对象角色的方方面面。作为社会工程人员，你伪装得越全面就越令人信服。一般情况下，伪装得越简单，说明技术越娴熟。

伪装，尤其是从互联网出现以来，越来越多地被恶意利用。我曾经看到过一件T恤上写着："互联网上，男人是男人，女人是男人，小孩子是等待着你的FBI探员。"虽然这是句调侃，但这种说法有一定的道理。在互联网上，你可以随心所欲地装扮成任何人。这种伪装技术多年来一直被恶意黑客用来攫取利益，而且不仅限于互联网。

在社会工程过程中，角色扮演或者假扮别人以达到目的有时是必要的。克里斯·海德纳吉或许没有一个技术支持人员或者一个进出口公司首席执行官那么大的影响力。当一个社会工程情形出现，有能力成为那个要伪装成的人是非常重要的。在一次讨论会中，我和世界知名的社会工程人员克里斯·尼克尔森（Chris Nickerson）聊到这个话题，他说到了一些我认为真正切中要害的观点。

尼克尔森说伪装不是扮演某个角色或者出演部分剧情，不是撒谎后不停地圆谎，而是真的成

为那个人。你的一丝一毫都是正在扮演的那个人。走路的方式、说话的方式、肢体语言都与那个人一样。我同意他的这个伪装哲学。一部令人感到绝无仅有的电影，往往是因为演员的出色表演，他们对于角色巧妙、精准的演绎让我们难分真假。

这在我的生活经历中得到过验证，很多年前我和妻子观看了布拉德·皮特出演的精彩影片《燃情岁月》。电影中他扮演一个自私的混蛋，拥有一个饱受折磨的灵魂，做了很多错误的决定。他的表演如此到位，以至于我妻子讨厌了这个演员好几年。他就是个很好的伪装者。

很多社会工程人员以为伪装仅仅是乔装打扮。衣着的确能起到作用，但伪装是门学问。通过伪装这种表演方式，可以整个变成另外一个人。要实现这一点，社会工程人员必须明确到底什么是伪装，作出计划，并演绎完美的伪装，这样才有可能成功。本章将涵盖伪装的各个方面。首先会讨论伪装的确切定义。接着讨论作为一名社会工程人员如何去伪装。最后，会把这些结合起来，通过几则故事去展现如何有效地应用伪装。

4.1 什么是伪装

伪装的定义是创造虚构的场景以劝说目标受害者泄露信息或者作出某种行为。这绝不仅仅是说谎那么简单，在某些案例中有可能是创造一个全新的身份，然后用这个身份去获取信息。社会工程人员可以利用伪装技术扮演从事某些特定工作的人和他们从未担任过的角色。伪装没有固定的万能模式，社会工程人员必须在“职业生涯”中创造很多不同的伪装。所有伪装都有一个共同的特点：研究。娴熟的信息收集技术是伪装成功的关键。打个比方，如果目标不需要外部技术支持，即使我们将技术支持人员模仿得再完美也无济于事。

伪装不仅可用于社会工程中，也能在生活领域发挥作用。销售人员、公共演讲者、算命者、神经语言程序学专家，甚至是医生、律师及临床医学家等，都需要使用一定形式的伪装。他们都需要创造一个适宜人们泄露隐私信息的场景。社会工程人员和其他伪装使用者的差异在于目标的设定。社会工程人员必须完全变身为伪装的角色，而不仅仅是装腔作势。

只要审计或者社会工程没有结束，都应该继续伪装。我就进入过角色，我的同事也是，有人在事情过后还沉浸在扮演的角色中。无论去什么地方，都要是所扮演的角色。此外，很多专业社会工程人员具有多个在线身份、社交网站的身份、电子邮件和其他账户，可供伪装的时候用。

在我参与的社会工程播客节目中，曾经就该话题采访过电台明星汤姆·米施克（Tom Mischke），详细信息参见www.social-engineer.org/episode-002-pretexting-not-just-for-social-engineers/。电台主持人必须精于伪装，因为他们只能透露宜于发布给公众的信息。汤姆在这方面很在行，绝大多数的听众都认为自己“了解”他，像朋友一样。他被邀请去参加婚礼、纪念日甚至是生日聚会。汤姆是如何完成如此神奇的伪装的呢？

答案就是不断练习。他给自己安排了很多很多的练习。他告诉我，他会制定出“表演对象”并且勤加练习——使用他们的发声方式，像他们一样坐立，甚至学习他们的穿着。好的伪装只能源于不断的练习。

要记住非常重要的一点：伪装的质量与所收集的信息质量有直接关系。信息越多，信息的质量和相关性越高，越利于我们的伪装，也就越容易成功。比如，如果一家公司只使用内部技术，或者将技术外包给一两个员工的小企业，那么经典的技术支持人员伪装就会完全失败。当别人质疑你的真实身份时，尽可能表现得自然，这直接取决于你对伪装是否能够运用自如。

现在你已经了解如何利用这项技能了。下面介绍伪装的原则以及如何应用这些原则来计划出令人信服的伪装。

4.2　伪装的原则和计划阶段

像其他技术一样，伪装也有一定的原则可以遵循。下面列出了一些原则。当然，并不是说就只有这些，还可以继续添加，只是这些原则体现了伪装的本质。

- 调查越充分，成功的几率越大。
- 植入个人爱好会提高成功率。
- 练习方言或者表达方式。
- 很多时候，如果低估了电话的作用，可能会减少社会工程上的投入程度。不过对社会工程人员来说，使用电话并不会减少精力的投入。
- 伪装越简单，成功率越高。
- 伪装必须要很自然。
- 为目标提供逻辑结论或下一步安排。

下面各小节将详细讨论每一条原则。

4.2.1　调查越充分，成功的几率越大

这个原则不言自明，但还是值得多次强调，因为收到的成效直接和调查的广度与深度相关。正如第2章里讨论的那样，这是社会工程成功的关键。社会工程人员掌握的信息越多，实现有效伪装的机会就越大。还记得第2章中讲述的我的导师马蒂·阿哈罗尼的故事吗？他是如何说服一位高管访问他的集邮网站的？乍一看，对这家公司的进攻之路应该和金融、银行、融资或其他类似的事情有关，因为这是一家金融机构。马蒂做的调查越多，越觉得伪装成一个集邮册出售者最为合适。找出高管的兴趣所在，让马蒂可以轻易地入侵这家公司，而且确实奏效了。

有时候细节决定成败。记住，没有不相关的信息。收集信息时，寻找故事、物品或者个人的

特点也是很不错的主意。利用目标个人的性格或者情感依托可以使你离成功更近一步。如果社会工程人员发现首席财务官每年都向一个儿童癌症研究中心捐赠一笔资金，那么伪装时涉及一个与此有关的筹款活动极有可能奏效，尽管这听起来有点无情。

问题是恶意的社会工程人员会不假思索地利用人们的同情心进行伪装欺诈。在2001年9月11日纽约双子大楼被攻击之后，很多恶意黑客和社会工程人员利用人员伤亡为自己牟利，他们设立网站，发送邮件给目标的计算机，并成立虚假基金，利用人们的慈善之心骗钱。在2010年智利和海地发生地震之后，同样的事情再次发生，很多恶意社会工程人员建立网站，发布地震活动或者失踪人员的信息。这些站点利用恶意代码导致人们的电脑中毒。

这类活动在某个电影明星或者歌星死后会更加猖獗。搜索引擎优化和市场营销天才会在几小时内让搜索引擎将他们的文章置于首页。恶意的社会工程人员同营销天才一起建立含有对搜索引擎优化的恶意站点，提升搜索引擎排名，从而利用人们对搜索引擎的不断关注来吸引大家访问这些站点，他们就会获取信息或者传播病毒。

有人会利用他人的不幸来牟利，是这个世界的可悲事实，这就是我所说的本书涉及的黑暗角落之一。作为一名社会工程审计人员，我可以利用一个雇员的感情向对方公司展示，表面上的好意会让这名职员泄露公司宝贵的商业运作数据。

所有这些例子都明确地表达了一点，社会工程人员信息收集和调查过程执行得越好，他促进伪装成功的几率就越高。

4.2.2 植入个人爱好会提高成功率

通过个人爱好去提高社会工程的成功率听起来很天真，但是有助于让目标信服你。如果开始时宣称自己在某一方面很擅长，最终却显示出这方面知识的匮乏，这绝对是毁掉信任关系的最快方式。作为一名社会工程人员，如果你从没见过服务器机房，没有拆过电脑的话，伪装成一个技术人员是很容易失败的。伪装中加入自己感兴趣的话题和活动，从而能够侃侃而谈，会使你显得聪慧而自信。

自信有助于说服目标相信你就是你宣称的那个人。某些伪装（例如集邮爱好者和核弹研究人员）需要更多的知识以让他人信服，这里我们又不得不提起前期研究。有时候伪装则比较简单，只要看一些网站或者读一本书就足够了。

对于社会工程人员来说，获取知识、研究感兴趣的话题，这是非常重要的。在伪装时，你可以聊故事、观点和工作，也可以聊你很了解的某种兴趣爱好，或者是一些谈起来很舒服的话题，看看这些能否奏效。

汤姆·G. 史蒂文斯（Tom G. Stevens）博士说："记住，你的自信心始终与任务和自身处境密切相关。不同情况下，我们的自信心是不一样的。"这种说法很正确，因为自信心直接跟

别人如何看待你这个社会工程人员有很大关系。自信（只要不是自大）可以建立信任和默契，而且让人感觉很放松。尽量让目标谈论你感到舒服的话题，然后你就可以自信地发挥，这点很重要。

1957年，心理学家利昂·费斯廷格（Leon Festinger）提出了认知失调理论。该理论认为，人们倾向于协调自己的信仰、观点乃至几乎所有的认知。如果态度和行为之间存在不协调，就必须要修正这种不协调。费斯廷格博士提出有两个因素会影响这种不协调的强度：

- 不协调的信念的数量
- 每个信念的重要性

随后他提出3种消除这种不协调的方法（每个社会工程人员都必须竖起耳朵听）：

- 降低不协调信念的重要性
- 增加更多的协调信念以超过那些不协调的信念
- 改变那些不协调的信念以使它们协调

社会工程人员如何利用这些信息呢？当伪装的角色需要你表现自信的时候，表现得不自信就会很自然地产生不协调。这些不协调引发各种红色警告，给你们之间的默契、互信和下一步进展带来障碍。这些障碍会影响目标人物的行为，他们会设法平衡自己不协调的感受，这样你的伪装就失败了。

避免这种情况发生的一种方法，是加入更多的协调信念以使其数量超过那些不协调的。目标对你的伪装角色有何期待呢？了解这些可以让你通过行动、谈吐和态度去迎合目标人物的思维和情感，从而建立起信念系统，让他们忽略任何值得怀疑的地方。

当然，一个技术娴熟的社会工程人员同样可以将不协调的信念变协调。虽然这很棘手，但是这项强大的技巧确实值得拥有。有可能你的伪装和目标的构想不一致。你可以回想一下《天才小医生》（*Doogie Howser, M.D*），豪斯医生很年轻，这和角色设定的顶级医生似乎不相符。这是个不协调的信念，但是他的渊博知识和行为又让“目标”认为这是协调的。就像之前的例子，社会工程人员可以通过观点、行动，尤其是知识，让他的伪装和目标的认知达成一致。

2010年举办的第18届Defcon峰会上，我见证了这样一个案例。我是社会工程夺旗竞赛（Capture the Flag，CTF）的组织者之一。我们发现很多选手伪装成内部雇员。当问到他们“你的工号是多少？”时，不成熟的社会工程人员会很紧张，要么回答不出要么直接放弃比赛，然而一个训练有素的社会工程人员却不会让目标产生任何不协调的想法。他会随口说出一个在网上找到的工号，或者用其他方法说服目标没必要提供工号信息，以此来消除目标的疑虑。

看似我们在以很专业的口吻解答非常简单的问题，然而，你必须得明白：伪装的方法虽多，但也是有限度的。请明智地选择适合你的那一种。

4.2.3 练习方言或者表达方式

学会用不同的方言与人沟通会给人留下深刻的印象。受居住地的限制，要学会说一种不同的方言或者口音需要一些时间。不是说不可能，只是学会像美国的南方人那样慢声细语地讲话或者学会亚洲人的口音会非常困难。有一次我参加一个国际营销组织举办的培训课程，他们提供的一些统计数据说明，70%的美国人更喜欢聆听一个英式发音的人讲话。我不确定这个统计数据是否属实，但是我会说我喜欢自己的口音。那个课程之后，我听说不少参加课程的人开始练习英式发音了，他们的发音真的很糟糕。我在英国有一个好朋友，名字叫乔恩，当他听到美国人试图去模仿英国口音来表演《欢乐满人间》时非常生气。如果他听到我们组说的英式发音，估计会气炸了。

这个课程让我明白，即便统计学告诉我们哪一种口音更利于销售使用，或者是因为你要到南方或者欧洲去做社会工程，这些都不意味着你可以轻易学会当地的口音。在存疑的时候，就扔到一旁。如果不能让你的方言完美、自然流畅，就不要去尝试。演员们为了和角色的口音一致并且发音清楚，需要专门的声乐教练及培训课程来练习发音。克里斯蒂安·贝尔（Christian Bale）是威尔士人，但是想从口音中辨别出来这点非常困难。在他大多数的电影里，他听起来并不像英国人。而电影《莎翁情史》中的格温妮丝·帕特洛（Gwyneth Paltrow）的英式口音就相当明显。

大多数的演员有方言教练帮助他们完善发音。因为大多数的社会工程人员请不起方言教练，所以可以看一些讲方言发音基础知识的书，比如伊万杰琳·玛琪琳（Evangeline Machlin）的《舞台方言》（*Dialects for the Stage*）。虽然这本书的出版时间比较早，但是包含了很多很棒的建议。

- 找到你想学的方言的例句听，像《舞台方言》这种书常常是附带录音带的，里面有多种方言。
- 努力跟着录音带说，学里面人的发音。
- 在感到自信以后，用该方言说话并录下，以便在事后听的时候纠正发音。
- 营造一个场景并和伙伴进行练习。
- 在公众场合用该方言说话，看看别人是否觉得可信。

世上有无数种方言和口音，我个人找到了一种很有用的方法，就是写下我要讲的话的音调。这样我可以练习朗读，并且记住大意，让我的口音更自然。

这些建议可以帮助社会工程人员掌握或者至少是熟练使用另一种方言。

即使不能掌握另一种方言，学会工作领域的专业表达方式也可以使情况有所改观。在公共场合听两个人交谈是一个好主意，餐厅、购物广场或者任何能找到一群人坐在一起聊天的地方都是绝佳的场所。仔细地听人们交谈所用的短语或关键词。当你听到他们在一些对话中运用的词汇时，可以考虑把它们纳入到你的伪装中，使其更可信。同样，这也需要研究和勤加练习。

4.2.4　使用电话不会减少社会工程人员投入的精力

最近几年，互联网开始主导某些“不需面对面交流”的社会工程活动。然而，在过去，电话是社会工程中不可或缺的一部分。由于这种转变，很多社会工程人员不再花时间和精力去探究“打电话”这件成功利器。

这里想说明的是，电话仍然是一种非常强大的社会工程工具，不该因为互联网的非人格化性质而减少对它的使用。

很多时候，社会工程人员在策划电话攻击时的想法会有所不同，因为利用互联网看起来更简单一些。要记住，在使用电话进行社会工程时，要投入同等的精力、同等深度的研究和信息搜集，最重要的是同等水平的练习。我曾和一个小组一起练习利用电话进行攻击。我们研究了适宜的方法、语调、语速、音调以及措辞，然后过了遍剧本（通常一分钟左右的时间），开始了一个会话。第一个人打了电话，连线到某个人，刚开始的几句话就搞得一团糟。在彻头彻尾的尴尬和恐惧中他挂掉了第一通电话。这给我们上了很好的一课：话筒另外一头的人根本不知道你想说什么，所以你不会真的“搞砸”。练习会话可以帮助你学会处理那些意料之外的事，而这通常是由你不慎改变剧本所造成的。

如果没有一组人陪着你训练或磨练这些技能，你必须得有创造力。试一试给家人或者朋友打电话，看看你能在多大程度上操控他们。另一种练习方法是给自己录音，就像在打电话一样，然后重放一遍看看听起来如何。

我个人认为使用剧本大纲是很重要的。这里有个设想：想象你不得不给电话公司或者另外一个机构打电话。理由是他们搞错了一笔账单或者服务有问题，所以你打电话过去抱怨。在你跟客服解释以后，告诉他你有多失望，有多生气。客服没有为你提供任何帮助，他说：“本公司承诺提供最好的服务。请问还有什么需要帮助的吗？”如果电话另一端的人稍微思考一下他的问题，就会知道这样问有多傻，对吧？这就是使用剧本而不是大纲所导致的问题。大纲允许你有“艺术创造的自由”，让你在对话里中灵活机动，不必担心下面必须要发生什么。

使用电话提高伪装的可信度，是得到目标认可最快的方法之一。电话允许社会工程人员去“哄骗”或者假冒几乎任何事。看看下面这个例子。如果我想假装是在一个忙碌的办公室里给你打电话，我可以到www.thrivingoffice.com下载一段音频。这个站点提供了一个录音叫“忙”，另外一个叫“很忙”。它们的创作者称：“这个CD很有用，它包含人们可在一家公司听到的所有声音，让人们立即相信这是真实的场景。简单、有效而且质量有保障！”

这个句子就蕴含着社会工程的真谛——充斥着人们想要听到的办公嘈杂声。你发现这个CD能够满足你的预期，而且相当可信（至少在满足目标的预期后，他会是这样认为的），从而能够自动得到信任。

此外，伪造电话号码欺骗要相对简单一些。像www.spoofcard.com提供的服务或者一些自制的方法，都可以帮助社会工程人员改变来电显示的电话号码，让目标认为你是从公司总部、白宫或者当地银行打过来的。利用这些服务可以伪造出世界上任何地方的电话号码。

电话对于社会工程人员来说是非常有用的，养成使用电话的习惯，给予它足够的尊重，可以增强社会工程人员伪装的技能。因为电话是如此有效的工具，而且它的效力还将持续下去，所以必须在它身上花费相当的时间和精力，让它在任何社会工程场景中发挥作用。

4.2.5 伪装越简单，成功率越高

“越简单越好”的原则一点也不夸张。如果伪装有很多错综复杂的细节，以致忘记任何一个都会导致失败，那么就真的会失败。保持故事情节、事实和细节的简单性，会增强可信性。

人际欺骗领域有名的心理学家和研究人员保罗·艾克曼（Paul Ekman）博士，在1993年发表了一篇联合署名的文章，名为“失败的谎言”（Lies That Fail）。在那篇文章中他认为：

> 很多时候你没有时间去准备故事情节、进行练习和记忆。就算事前有很充分的预案，也有可能突然冒出一个不能预见的方向，说谎者不可能聪明到可以预见所有可能被问及的问题，也不可能准备所有的答案。仅有聪明的头脑是不够的，环境中不可预见的变化会导致原先有效的准备变得不可行。而且，即使不是为情势所迫改变方向，某些撒谎者也会由于记忆问题想不起前面的描述，结果不能快速一致地解答新的问题。

这个重要观点将为什么越简单越好解释得很清楚。如果伪装很复杂，努力去记住伪装的全部内容基本是不可能的，一个很小的错误就可能把你的伪装全部毁掉。伪装应该尽可能地自然、顺畅，应该容易记住。如果觉得很自然，那么回忆之前的事实和故事就不会是负担。

为了表明细节记忆的重要性，我想跟大家分享一则小故事。我曾经从事过销售领域的工作，被安排和一位销售经理一起共事、学习。我还记得他给我上的第一堂课。我们开车到客户的家门口，在下车之前，他看了看信息卡，告诉我：“记住，贝姬·史密斯（Becky Smith）发过来一个请求卡，要求补充保险。我们要用XYZ策略。仔细观察，好好学。”

在前3分钟里他称她为贝斯或贝蒂，每次他叫错名字，我都看到她有情绪波动，然后她会很轻地说：“是贝姬。”尽管我们已经给了她很大的优惠，但依然被拒绝了。她对于自己的名字总被说错很失望，所以对于听到的任何东西都不感兴趣，也听不进去了。

这个场景真实体现了保持简单的重要性。

除了记住事实之外，不过分追求细枝末节也很重要。一个简单的伪装允许故事发展，并且允许目标运用想象去填满空隙。不要试图将伪装设计得很精致，只要记住那些伪装中比较关键的小细节即可。

此外，还有一个有趣的花招：知名罪犯和骗子的一个常用伎俩是故意犯一些错。这个想法是基于“人无完人”而建立的，一些错误会让人感觉很真实。如果运用这个策略，得留心选择决定去犯的错误，虽然这确实让对话看起来更自然，但它增加了伪装的复杂性。少用这一花招，如果一定要用，尽可能地简单。

现在我用以前审计过程中使用过或看见过的例子将上面几点结合起来。通过打电话的良好诱导，一名社会工程人员知道了公司所用的清洁公司的名字。通过网上搜索，他找到了能打印出来的清洁公司的标识。有很多本地或者网上商店可以按照客人的要求将标识印在衬衫或帽子上。

对照模板调整了几分钟，他订购了一件衬衫和一个球帽，上面印有垃圾回收公司的标识。几天过后，穿着印有标识的衣服，带着一个写字夹板，这位社会工程人员来到了目标公司的保安亭旁。

他说：“你好，我是ABC垃圾回收公司的乔，我们接到你们采购部门的电话，要求派一个人来检查后面被损坏的垃圾箱。明天会来人收垃圾，如果这个垃圾箱无法修复，我会让他们带一个新的来。但是我得去后面检查一下。”

保安人员毫不迟疑地说：“好吧，你需要带着这个徽章过去。经过这里再绕到后面，就可以看到垃圾箱了。”

社会工程人员顺利拿到了通行证，对垃圾箱进行了长时间仔细的翻查，但是他还想扩大战果，试图进一步发现线索。他看着写字板说：“这里显示说要检修的不是食品垃圾箱，而是装纸张和技术垃圾的。到底会在哪里呢？”

“哦，照着我告诉你的路线，它们在第3隔间。”保安说。

“谢谢！”乔说。

简单的伪装，穿着有标识的衣服，带着“工具”（如写字板），并且故事情节简单而又好记。正是它的简单性和缺少细节使得这次伪装更加令人信服，进而发挥作用。

另一种惯用的伪装就是所谓的技术支持人员。只需一件Polo衫、一条卡其裤与一个小的电脑工具包。许多社会工程人员使用这种技术顺利进入了公司大楼，因为“技术人员”通常能不受监督地进入任何地方。同样的法则也适用于这里，即保持故事情节的简单会使这种伪装真实可信。

4.2.6　伪装必须显得自然

想要使伪装看起来自然一些，可以采用我前面推荐的大纲模式，而不是使用剧本方式。大纲模式下社会工程人员可以自由地发挥，使用详细的剧本则会太机械。伪装中可以加入社会工程人员感兴趣的项目或故事。假如每次有人问一个问题或做出一个论述，你都支支吾吾，需要深入地思考，而不能做出及时明智的回答，可信性就会因此大打折扣。确实，很多人都是思考后再说，

因此这并不是要求你立即答复，但是要有答案或者要找到一个没法回答的借口。比方说，有一次对方在电话中询问一则我不知道的信息。我就说："让我找找。"然后我迅速看了一遍，假装我是在大声询问同事："吉尔，麻烦让比尔给我份XYZ账户的订货单。谢谢！"

然后"吉尔"会拿来表格，我就可以得到需要的数据，而表格再也不会被提起。

下面列出了几条让伪装更加自然的方法。

- **不要考虑自己的感受**。这点很重要，因为通常在伪装时如果想太多就会融入更多的个人情绪，然后恐惧、不安或焦虑就会随之而来，这些都可能会导致失败。另外，你可能不会经历不安或焦虑，但会过度兴奋，这同样会使你犯很多错误。
- **不要把事情太当真**。当然，在生活中这就是一条好建议，而且同样非常适用于社会工程学。作为一名专业的安全人员，你有一份很严肃的工作，这是一件严肃的事情。但是如果不能笑对自己的错误，就可能会沉默不语，或者在处理后续的小事情时如临大敌。当然，我并不是建议你视安全如儿戏。但是，如果你将潜在的失败当做人生中巨大的失败，那么产生的压力恰恰会导致最坏的结果。只有正确看待小的失败，才能取得更大的成功。
- **学会找到相关信息**。我喜欢用"摆脱思维的束缚，融入这个世界"来描述这个理念，这是一个非常棒的建议。社会工程人员可能全力计划好了前3个步骤，但却遗忘了一个可能会使伪装土崩瓦解的关键细节。要始终留意身边出现的信息和状况，包括目标的肢体语言、说的话，微表情（第5章会详细介绍）等，然后将其应用到自己的行动中。
  同时，记住说话者能看出什么时候你没在认真听他说话。这会让很多人感到不爽，就算是无关紧要的句子，没有被听取也会招致不快。每个人都经历过自己的话被人当做耳边风，或许他们有各自正当的理由开小差，但这样做真的挺让人扫兴的。
  一定要注意听目标所说的话。集中注意力，你会听到一些对他们很重要的细节，同时也能够获取有助于自身取得成功的信息。
- **争取多积累经验**。在这本书里，你可能会反复看到一个词语，那就是练习。通过实践积累经验，能成就伪装也能识破伪装。有意识地、毫无目的地在和家人、朋友甚至是陌生人的交往中练习自然地伪装。抛开死缠烂打的方式，与他人展开简短的会话，可以使你在伪装的时候表现得更加自然。

这些方法绝对能使社会工程人员在伪装时处于优势地位。具备自然伪装的能力是一种天赋。本章前面谈及了我对汤姆·米施克的采访，他对表现自然持一种很有趣的看法。他说他在练习和准备的过程中，都会将"表现自然"作为一个目标。每次伪装前，他都会进行大量的练习，以至于足以使伪装自然得像是幽默与天赋的产物。

4.2.7 为目标提供逻辑结论或下一步安排

无论你相信与否，事实是人们都希望被告知下一步该做什么。想象一下，你去看病，医生走

进来给你检查了一番，并且在记录纸上写了一些东西，然后说："好了，下个月见。"这是让人无法接受的。就算是听到坏消息，人们也希望被告知下一步该做什么。

作为一名社会工程人员，你要离开目标时，可能需要他采取或不采取行动，或者你已经得到想要的，只需离开。无论是什么情况，都应给目标一个结论或不会令其怀疑的下一步安排。

就像医生给你检查了身体，然后没有任何指示就打发你回家。如果在社会工程中，伪装成技术支持人员进入一幢大楼，在复制好数据库之后一句话也不说就离开，会让每个人产生疑惑：到底发生了什么事？甚至有人可能会给技术支持公司打电话，询问是否还要他做什么，或者最坏的情况是让他们自己胡乱猜测。无论是哪种情形，这种一句话也不留的离开方式都是有问题的。哪怕简单的一句"我已经检查了服务器并且修复了文件系统，你们会发现系统在未来几天里运行速度会提高22%"，都会让目标觉得"他们的钱花得值"。

令社会工程人员感到棘手的是让目标在他走后采取行动。如果这一行动对完成社会工程审计非常关键，你会想要自己主动出手。比如在第3章中，我讲到在一个商业会议活动中收集信息的案例，如果想让目标给我发邮件，我会说："这是我的名片，你是否可以在星期一给我发一封邮件，详细介绍一下XYZ公司？"他可能会记得给我发，也可能一回办公室就把我忘得一干二净了，这样整个事件会以失败告终。也许这样说会更好："我非常想从你那里了解更多的信息。在周一时我可以给你打电话或者发邮件询问更多细节吗？"

你提出的要求也应该和自己伪装的身份相匹配。如果你伪装成技术支持人员，则不应该"命令"周围的人必须做什么或者不能做什么，因为你在为他们提供服务。如果伪装成UPS快递员，你就不应该要求进入服务器机房。

正如之前提到的，一次完美的伪装还需要很多的步骤，但是对于需要进行完全可信的伪装的社会工程人员来说，本章的内容已经足以为你夯实基础了。

你可能会问："好吧，你列出来这么多原则，那接下来该如何呢？"社会工程人员要如何做，才能在电话里或者与他人面对面的交流中，进行前期调研充分、可信、语气从容而简单的伪装呢？怎样才能得到想要的结果呢？欲知详情，请继续阅读本书。

4.3　成功的伪装

要学习如何进行成功的伪装，就需要了解那些曾经成功伪装过的社会工程人员的故事，学习他们是如何展开伪装的。当然，他们的伪装最后都被识破了，因此我们现在才能读到这些故事。

4.3.1　案例1：斯坦利·马克·瑞夫金

斯坦利·马克·瑞夫金（Stanley Mark Rifkin）一手策划了美国历史上最大的银行抢劫案（关

于他的相关信息，请参见www.social-engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer-furtherInfo.htm）。他是一名电脑极客，在他的小公寓里开了家电脑咨询公司，他的一个客户是给美国证券太平洋国民银行（Security Pacific National Bank）提供电脑服务的公司。坐落在洛杉矶的美国证券太平洋国民银行总部有55层，看上去就像一个用花岗岩和玻璃建成的堡垒。着深色制服的保安在大厅里巡查，隐藏的摄像机记录着每个来银行办理存取款业务的客户的一举一动。

这幢大楼看起来无懈可击，那么瑞夫金是如何在不携带任何武器、不动一分钱、不胁持任何人质的情况下带走1020万美元呢？

银行的电汇机制应该是很安全的，每笔电汇都必须输入密码，而且这个密码每天都会被强制修改，只有特定的人知道。密码被贴在安全房间的墙壁上，而且只有“特许人员”才可以进入这个房间。

前面提到的存档文件中是这样记录的。

> 1978年10月，瑞夫金来到了美国证券太平洋国民银行，银行工作人员理所当然地认为他是计算机工作人员。他坐电梯来到电汇室所在的D层。伪装成友好而且和蔼可亲的年轻人，他竟然进到墙上贴有当天密码的那个房间里。瑞夫金记住了密码，然后在没有引起任何怀疑的情况下离开了。
>
> 很快，银行电汇室的员工接到了迈克·汉森（Mike Hansen）打来的电话，他自称是该银行国际分部的员工。他正确地给出了当天的密码，要求为纽约欧文信托公司资金账户进行常规转账。整个过程没有任何引起怀疑的地方，所以美国证券太平洋国民银行就把钱打到了纽约银行的账户上。银行官员不知道的是，那个自称是迈克·汉森的男人其实是瑞夫金，他通过银行的安全密码盗取了1020万美元。

这个案件留下了许多可圈可点之处，但是现在我们把焦点集中到伪装上面来，仔细想想瑞夫金作案的细节。

- 为了能够在密码房间里不引起怀疑，他需要足够的自信和镇定。
- 提出汇款要求，他需要编一个足够令人信服的故事，而且需要考虑足够多的细节来自圆其说。
- 面对可能出现的问题，他要表现得足够自然。
- 为了不引起银行员工的怀疑，他说话要足够熟练和流利。

这些伪装必须经过细致的安排，考虑到每一个极其微小的细节。直到遇见了一个前同事，瑞夫金才被揭穿。瑞夫金被抓的时候，认识他的人都非常吃惊，甚至有人说：“他不可能是个小偷，人人都喜欢马克！”

很显然，他的伪装是很到位的。他的计划经过深思熟虑，安排周详，排练纯熟。他知道去那里的目的，并且每一步都做得很完美。站在陌生人面前时，他知道如何伪装。如果不是熟知瑞夫

金的同事看了新闻后把他指认了出来，他是不会被发现的。

更加令人吃惊的是，当瑞夫金被保释在外的时候，他又打算用相同的方法“抢劫”另一家银行，但是他的行为落入了政府侦查员设计的陷阱，他被抓住了，并且等待他的是8年的牢狱之灾。尽管马克是一个“坏人”，但是从他的故事中我们能够学到很多关于伪装的知识。他的伪装非常简单，完全是用他熟悉的事情来打造精彩的故事情节。

马克的计划是把偷出来的钱变成不可追溯的钻石。为了实现这一目标，他首先需要成为一名银行雇员以拿到钱，然后变成一个钻石收购商将这些现金“洗掉”，最后通过把钻石卖掉，获得可以使用的、无迹可寻的、干净的现金。

他的伪装不涉及装扮和说话方式的变化，却要依次扮演银行工作人员、钻石采购商和钻石销售商。这其中要完成3次、4次甚至5次的身份变化。他做得非常好，基本上欺骗了所有人。

马克知道他的目标是哪些人，并且按照我们前面提到的所有规则来一步步实现他的计划。当然，他的行为是不可宽恕的，但是他的伪装天赋却是令人羡慕的。如果把天赋用到恰当的地方，他很可能会成为一位伟大的公众人物、销售员或者演员。

4.3.2　案例2：惠普

2006年，《新闻周刊》发表了一篇非常有趣的文章（详见www.social-engineer.org/resources/book/HP_pretext.htm）。故事基本上是这样的：惠普公司的董事长帕特里夏·邓恩（Patricia Dunn）女士雇用了一个专业的安全团队，这个团队又雇用了私家侦探，私家侦探利用“伪装”技术获取了通话记录。这些聘来的专业人士实际上伪装成了惠普的董事会成员及新闻记者。这一切都是为了找出惠普队伍中可能的泄密者。

邓恩女士希望获得董事会成员和一些新闻记者的通话记录（不是惠普公司内部的电话记录，而是这些人家中或者手机的通话记录），来查证她认为可能的泄密者。《新闻周刊》是这样写的：

> 5月18日，在加州帕洛阿尔托的惠普总部，邓恩在董事会上扔出了她的炸弹：她已经找到了泄密者！据在场的惠普董事汤姆·珀金斯（Tom Perkins）透露，邓恩展示了监视方案并且指出了那个董事，该人承认他就是CNET的泄密者。那名董事的身份至今还没有向外界透露。他道了歉，但之后对其他董事说：“我原本打算告诉你们所有的事情，为什么你们没有问过我呢？”珀金斯说，随后那名董事被请出了董事会议室。
>
> 这个事件中值得注意的是那个被称为“伪装”的话题。
>
> 惠普的这一事件还将公众的注意力吸引到了安全顾问为获得个人信息所采用的不合理的手段上。在外部顾问团发给珀金斯的一封内部邮件中，惠普承认他们通过有争议的“伪装”技术，获得了将那个泄密者和CNET联系在一起的书面记录。《新闻周刊》获

得了这封内部邮件的内容。美国联邦贸易委员会（FTC）认为这个技术涉及使用“欺骗手段”来获得他人的非公开信息：通话记录、银行卡和信用卡账号以及社会保险号等。

就拿案例中的电话公司来说，通常情况下伪装者会将自己伪装成客户，因为这些公司很少需要你提供密码，伪装者仅仅需要一个家庭住址、账号和诚恳的请求便能获取账号的详情。FTC的网站披露，伪装者会将这些信息卖给持证的私家侦探、金融贷款者、潜在的诉讼当事人以及对配偶有疑心的人，甚至卖给那些试图窃取资产或者骗取信贷的个人。FTC声明，伪装“是违法的”。FTC和若干州的检察长已就涉嫌违反联邦法和各州法律的欺诈、失实陈述及不公平竞争等行为对伪装者进行指控。惠普公司的董事之一，威瑞森（Verizon）公司的总裁拉里·巴比奥（Larry Babbio）已经以书面形式提交了打击伪装者的各种措施。

（如果你对具体内容感兴趣，可以在下面的链接中找到2006年的《电话记录隐私权保护法》：http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4709enr.txt.pdf。）

最终的结果是刑事控诉不仅针对邓恩女士一人，她所聘请的顾问也被指控。你也许会疑惑：“怎么可能对他们进行指控呢？他们是签了合同、被雇用来进行这些测试的啊。”

很简单，分析一下他们获取信息的途径以及内容，就有了答案。这些顾问拿到了惠普董事会成员和记者的姓名、地址、社会保险号、通话记录、电话账单记录以及其他一些信息。他们甚至使用一个记者的社会保险号建立了在线账户，以获取其私人通话记录。

惠普提交给其律师和内部法律人员的一份机密文件（详见www.social-engineer.org/resources/book/20061004hewlett6.pdf）的第32页列出了汤姆·珀金斯和惠普董事会成员的交流内容，其中包含一些有关伪装的内容。其中用到的部分策略列示如下。

- 他们将自己伪装成电信运营公司以非法地获取通话记录。
- 使用被调查者的身份来获取他们的私人通话记录。
- 利用非法获得的姓名、社会保险号和其他信息建立在线账户，从而获得他们的通话记录。

2006年9月11日，美国众议院能源和商务代表委员会给邓恩女士发了一封信（详见www.social-engineer.org/resources/book/20061004hewlett6.pdf），要求其提供所取得的所有信息。以下是他们列出的信息类型。

- 所有公布的和未公布的电话号码；
- 信用卡账单；
- 客户姓名和地址信息；
- 公共事业账单；
- 寻呼机号码；
- 手机号码；

- 社会保险号；
- 信用报告；
- 邮政信箱信息；
- 银行账户信息；
- 资产信息；
- 其他消费信息。

所有这些信息都是采用社会工程领域的灰色方法取得的。虽说是受雇做这种工作，但是他们所做的事情符合伦理道德吗？许多专业社会工程人员均不敢越雷池半步。从这一经典案例中，我们也能吸取一些教训：作为一名专业的社会工程人员，你可以模仿那些心存恶意的社会工程人员的方法和思维方式，却决不能堕落到他们那种地步。那群顾问犯的错误是：他们被授权去伪装、社会工程和审计惠普，但并没有被授权去审计美国电话电报公司（AT&T）、Verizon公司及公用事业公司等。在伪装的过程中，必须有明确的概要并且规划出哪些法律漏洞可以被利用，而哪些底线是决不能触碰的。

假如你是一名社会工程审计人员，可以就惠普这个案例展开关于政策、合同和原则等系列讨论，但这些内容不属于本章的讨论范围。使用本章所列出的原则有助于你作出决定，而且这些决定不会让你惹祸上身。

伪装成危险的、怀有恶意的身份盗用者，是社会工程渗透测试中合法的方式。测试、检查和验证你的客户的雇员不会落入恶意社会工程人员的陷阱，也可以帮你防御成功的伪装者。

4.3.3　遵纪守法

2005年，《私家侦探》杂志获得了对美国联邦贸易委员会金融实践部副主任乔尔·温斯顿（Joel Winston）的采访机会。他所在的部门专门负责规范和监测那些伪装行为（采访内容详见www.social-engineer.org/resources/book/ftc_article.htm）。

此次采访的要点列示如下。

- 据美国联邦贸易委员会定义，伪装是指使用诈欺、欺骗或者误导性问题来取得银行或消费者的信任，从而拿到财务情况等信息。
- 在美国联邦贸易委员会看来，使用已经获得的信息来确认目标身份的真实性是合法的，即便在该过程中采用了欺骗手段。但是社会工程人员不能利用这些从金融机构获取信息。
- 通过诈欺性的商业行为来获得电话清单或者手机通话记录被认为是非法的伪装行为。

美国联邦贸易委员会的官方网站澄清了本次采访的一些内容，并提供了如下补充资料。

- 任何使用虚假的、伪造的或欺诈性的陈述或文件，从金融机构窃取客户信息，或者直接从金融机构的客户那里骗取其信息的行为都是非法的。

- 任何使用伪造的、假冒的、丢失的或被盗取的文件，从金融机构窃取客户信息，或者直接从金融机构的客户那里骗取其信息的行为都是非法的。
- 任何指使他人使用虚假的、伪造的或诈欺性的陈述或文件，或者使用伪造的、假冒的、丢失的或被盗取的文件，从他人处骗得客户信息的行为都是非法的。

虽然联邦贸易委员会的焦点是金融机构，但其列出的指导方针也能提醒你在美国哪些伪装是违法的。了解当地的法律并且确保不会违法，对于专业社会工程人员来说非常必要。2006年，美国联邦贸易委员会对《FTC法案》第五条进行了补充，明令禁止使用伪装技术获取电话记录。

前面惠普案例中的五个私家侦探之一被指控为蓄意窃取身份罪，这项罪名相当严重。

保持伪装的合法性需要专业社会工程人员不懈的努力和研究，并且明确地计划要使用什么样的伪装。

排除之前提到的法律因素，利用可靠的伪装手段进入目标公司是最快的途径之一。然而，从本章的介绍也能够看出，伪装本身是要讲究天赋的，不只是戴上假发或者眼镜去冒充别人那么简单。

4.3.4 其他伪装工具

伪装时还有其他一些可利用的工具。

道具有助于让目标相信你的伪装。比如，车辆的磁性标志、配套的制服或装备、工具或者其他手提设备，还有最重要的——名片。

在我最近飞去拉斯维加斯出差的时候，名片的重要性震撼了我。我的笔记本包通常会被一遍又一遍地扫描，然后做除尘（炸弹尘埃或者别的危险物品）。我对这种安检从不反感，因为它们避免了我在空中被炸飞的可能，这点让我很高兴。

然而，我意识到90%的情况下，我都会引起安检人员的额外注意。这次出行比较特别，我忘记将开锁套装、RFID扫描器、4块额外的硬盘、万能钥匙（参见第7章）和一些用来进行无线入侵的工具从随身的笔记本包里拿出来。当这些东西从扫描仪器中通过时，我听到X光仪器的女操作员说："这些是什么？"

随后她叫来一个男同事看了看屏幕，他说："我也搞不清那些到底是什么。"他继而环顾四周，看到我在笑，便问道："是你的吗？"

我和他一起走到桌旁，他倒出我的RFID扫描器和专业开锁套装，问道："你怎么会有这些东西？干吗用的？"

显然我被问到了，但是在最后一秒钟我决定尝试一下。我拿出一张名片，说道："我是为网

络、建筑和人们做各种测试的安全专家，这些都是我的工具。”说着我递给他一张名片，他看了大概5秒钟说：“哦，不错。谢谢你的解释。”

他把我的东西整齐地放回去，把包拉好，就让我走了。通常，我还得通过炸弹探测器、小除尘机，然后被搜身，但是这次我得到的却是一句“谢谢”和快速放行。我开始分析原因，唯一的不同就是我递给他一张名片。当然，我的名片不是那种在线印刷的廉价商品，但令我没想到的是，这张名片在关键时刻充当了许可证，能够有效证实我的描述。

在接下来的4次飞行中，我特意把我所有的“黑客”装备放进我的包里，然后拿一张名片在兜里。每一次在安检时被问及这些东西时，我就递上名片。毫无例外，每次他们都向我道歉，把我的东西整齐地装回去，然后放行。

如果将我的经历想象成伪装。一些小细节可以让我说的话可信度大增，让我看起来正当并值得信任，而这一切只需要一张卡片，就可以让人相信我说的都是事实。千万不要低估名片的作用。友情提醒：印刷粗糙、看起来寒碜的名片的效果恰恰相反。一张背面印有“免费”广告的名片在专业伪装中不会起任何作用。不过，也没必要在这上面花费300美元，你完全可以用不到100美元让网上名片打印店打印少量精美的名片。

另一个需要认真对待本章的理由是，伪装通常是专业身份窃贼开始入手的第一步。鉴于身份盗用在最近犯罪中出现得比较频繁，知道它的原理并且能够有效鉴别，对于消费者、商务人员和安全专家来说都有很大的必要性。如果你是一位安全审计师，必须帮助客户提防这类威胁，并且针对可能的漏洞考验、测试他们。

4.4　小结

前文系统地介绍了伪装，并且提供了真实的案例。除此之外，本章还提及心理学原则也会影响伪装的方方面面。下一章将着重介绍和讲述专业社会工程人员如何使用心理战术成为精神控制专家。这点可以让每个社会工程人员向成功迈进一大步。

第 5 章
心理战术：社会工程心理学

我们看待事物的方式而不是事物本身，决定着一切。
——卡尔·古斯塔夫·荣格（Carl Gustav Jung）

在好莱坞电影和电视剧中，骗子和司法办案人员总是被描绘成具有神秘的才华。他们具有逃脱一切追查的能力，通过他人的眼睛就能识别出对方说的是谎言还是事实。通常我们会看到这样的场景：警察凝视着疑犯的双眼就可以判断出他是否在说谎，或者通过三言两语骗子就能令受害者拿出毕生积蓄。电影可能会让你相信操纵技术以及“让人们做任何事”都看似合理，甚至很简单。这些场景真的只是虚构出来的吗？可能获得影片中描绘的这种类似幻想的能力吗？

本章涉及的内容可以写成一本书，我将这些丰富的信息概括成了一些准则，而这些准则将改变你和他人打交道的方式。本章涉及的一些话题是以一些极为聪明的研究者在各自领域的研究成果为基础的，这些话题中讨论的技巧也都在社会工程的环境下经过了缜密的测试。例如，微表情这一话题就是以世界著名的心理学家和研究学者保罗·艾克曼博士的研究成果为基础的，他利用自己的天赋开发出的解读人们面部表情的技术，改变了司法人员、政府官员、医生以及普通人与他人交往的方式。

神经语言程序学的鼻祖理查德·布兰德勒（Richard Brandler）和约翰·葛瑞德（John Grinder）提出的一些理论，改变了人们对思维模式和语言重要性的认识。这些都是相当具有争议的领域，本章将揭开其神秘面纱，并且讲解其在社会工程中的应用。

一些最优秀的审讯者开展了培训工作，并开发了相关的框架，帮助执法人员学习怎样有效地审讯嫌疑人。这些原则和方法具有深厚的心理学基础，学习这些方法可以正确解读目标的思维方式，攻破他们的心理防线。

正确地解读人们说话、手势、眼神和面部表情中的信号，可以使你看起来像一位精通读心术的人。本章将细致阐述这些技巧，以供专业社会工程人员使用。

亲和力是销售培训人员和销售人员经常提到的字眼，这是获取信任、显示信心的一个非常重要的方面。本章将介绍如何在短时间内与目标人物建立友善的关系，真正提高社会工程人员的技能和水平。

本章以我个人对人类思维攻击的研究成果收尾。缓冲区溢出通常是由黑客编写的程序，通过宿主程序的正常使用，可以利用它执行通常带有恶意目的的代码。一旦运行起来，程序会按照黑客预先设定好的步骤执行任务。那么如果可以在人类的大脑中执行“命令”，让目标按照我们的要求行动、给出我们想要的信息，会怎么样呢？这样是不是就可以证明人的思维是可以被操纵的呢？

这一强大的信息当然也会被用来达到恶意目的。我以这种方式将此信息公布于众，目的在于揭开“坏人”的面纱，剖析他们的手段、思路和准则，然后一一进行分析，让读者学会如何识别他们的真面目。将这些技术公开出来，有助于大家轻松识别、抵御及缓解这种攻击。

学习本章所涉及的数据和准则需要读者不停地转换思维。模仿、学习并研究这些方法不仅能够提高你的安全能力，还能够改变你和他人沟通及交流的方式。

当然，本章并不能涵盖这些技巧的所有方面。我提供了一些有助于你强化这些技能的链接或者建议。本章不仅是行为指南，更为社会工程奠定基础，为你指明方向，从而在日后不断强化社会工程技巧。

社会工程技巧的学习并非一蹴而就之事，所以要有耐心。这些技巧的学习需要花费几年的时间，如果要达到专业级别，更需要很多实践的磨练。当然，你可能很快掌握一些特定方面的技巧，如果不能很快掌握的话，也不要放弃。只要功夫深，铁杵磨成针。

在进入本章的正式内容之前，下面将会做一些准备工作，说明为什么这些原则会起作用，以及它们是如何起作用的。我们必须要理解人类的思维模式。在对人们吸收和处理信息的模式理解得更为透彻后，你就能开始理解这一过程背后的人类情感、心理学和身体表示。

5.1　思维模式

要改变某人的思维方式，必须要理解人们的思维方式和思维模式。逻辑上，这是进行这方面社会工程尝试的第一步。

听上去好像我们得成为心理学家或者神经学家才能理解人们思维的方方面面。纵然那会有一定的帮助，但其实没那个必要。通过一些研究和实际应用，就能深入人类思维的内部工作机制。

2001年8月，美国联邦调查局（FBI）发布了一份司法公告（详见www.social-engineer.org/wiki/archives/ModesOfThinking/MOT_FBI_3of5.htm），其中包含一些人类思维模式的深入阐述，具体如下。

> 让客户认可你的非言语行为、用客户认可的语言表达方式，并且在音量、语调和方言上相匹配，这样通常可以免吃闭门羹。

上面这句话虽简单，但是其中包含的内容却很多。一般来讲，如果能够迅速摸清目标的主导思维模式，然后通过微妙的方式进行确认，就可以令其在告知你哪怕是私密信息时，降低戒备，打开心扉。从逻辑上来讲，这时也许你会问："怎样才能识别目标的主导思维模式呢？"

即使问目标自己这个问题，也不一定能够得出一个清晰的答案，因为很多人并不清楚自己到底是何种思维模式。因此，社会工程人员必须掌握特定的工具才能识别他人的思维模式，然后快速切换到对应的模式。方法和途径有现成的，但是首先必须要了解其基础。

5.1.1 感官

对于认知的价值问题，哲学家已经争论了几个世纪了。有些人甚至认为，现实并不是"真实"的，它只是我们的感官带给我们的认知。就个人而言，我并不赞同这种思想，但是我相信这个世界是通过感官进入我们的大脑的。人们通过解释这些感官获得对现实的认知。传统的分类方法中，感官通常分为5种：视觉、听觉、触觉、嗅觉和味觉。

人们倾向于钟爱这些感官中的一种，也就是说某种感官会占据主导地位，这也是人们记住事物的方式。通过一个练习就能确定自己的主导感官，闭上眼想象你清晨起床的画面，你能记得的第一件事是什么？

是温暖的阳光照在脸上的感觉吗？是配偶或小孩叫你的声音吗？你清楚地记得楼下咖啡的香味吗？抑或是嘴里并不清新的口气，提醒你需要刷牙了？

当然，这一实验并不能完全确定，可能要尝试好几次才能真正意识到自己的主导感官。我曾经和一对夫妇说起过这一概念，他俩的反应很有意思。妻子醒来的第一反应是看看时钟，担心自己快迟到了，而丈夫则是每次都翻个身，发现妻子不在身旁。几个问题之后，基本上可以确定丈夫是动觉类型的，或者说其主导感官是触觉，而妻子则是视觉占主导地位。

以上只是测试，实际工作中你不可能直接走向目标说："闭上眼，告诉我今天早晨起床后你做的第一件事是什么。"除非你伪装成家庭医生，否则肯定会吃闭门羹。

那么，如何才能在避免尴尬询问早晨起床习惯的情况下得知目标的主导感官呢？

5.1.2 3种主要的思维模式

尽管我们有5种感官，与思维模式相联系的只有其中的3种：

- 看到，也就是视觉思维者
- 听到，也就是听觉思维者
- 触到，也就是动觉思维者

每种感官都有各自起作用的范围，或者说有各自的次感元。声音太大或者太轻？光线太亮或者太暗？环境太冷或者太热？拿实际例子来说：直视阳光会感觉太过刺眼，喷气式发动机的声音太过震耳，零下30度（华氏）感觉太冷等。伊万·巴甫洛夫做过一个实验，每当给狗喂食时，他就摇手铃。最后狗一听到铃声就会流口水。然而，大多数人不知道的是，伊万更为感兴趣的是次感元引起的生理和情绪反应。有趣的是，铃摇得越大声，狗的口水流得越多。次感元的范围变化引起了身体的直接变化。欲详细了解巴甫洛夫的研究和他的全部演讲，请参见www.ivanpavlov.com。

尽管人和狗有很大的不同，巴甫洛夫的这项研究对于理解人们的思维模式还是很有价值的。我们中的很多人可能同时具备3种思维模式，但是占据主导地位的只有一种——“响声”最大的那个。甚至在主导思维模式下，主导感官的深度也会有所变化。

下面我们将深入地探讨每种思维模式的一些细节。

1. 视觉

大多数人通常都是视觉思维者，这种人通常记得的是事物的面貌。他们能够清晰地记住场景——颜色、纹理及光线的明暗等。他们能够清晰地描述过去的事件，甚至能构建未来事件的图像。当面对一些事物的时候，他们需要看到一些东西才能作决定，因为视觉输入直接与他们的决策相关联。很多时候，视觉思维者会依据在视觉上吸引他们的东西，而不是对他们来说真正“更好”的东西来作出决定。

尽管男人更可能是视觉思维者，但并不是说所有男人总是视觉导向的。虽然视觉营销或者视觉效果通常会对男人有吸引力，但不要以为所有男人都是视觉思维者。

视觉思维者在谈话中经常使用特定的词汇，例如：

- “我明白你的意思。”
- “我看那挺好。”
- “我大概有点印象了。”

对于视觉思维者来说，主导感官的工作范围具有一定的特征，通常这些也称为次感元。例如：

- 光线（明/暗）
- 尺寸（大/小）
- 颜色（黑白/彩色）
- 运动（快/慢）
- 焦点（清晰/模糊）

尝试在没有视觉输入的情况下与视觉思维者进行争论、协商，向其推销，操纵或者影响他，基本上会毫无效果，至少会非常困难，因为视觉思维者需要视觉输入才能作出决定。

2. 听觉

听觉思维者会记住事件的声音。他们会记住闹铃声音太大、女人的窃窃私语、孩子甜美的童声或者家犬惊悚的吠声等。对声音敏感的人通过倾听能够学得更好，而且相比于用眼睛看，别人告知他们事情时，他们能够获取更多的信息。

因为听觉思维者总是能记住事物发声的方式，或者说声音能够唤起他们的记忆，所以他们经常使用这样的表述：

- “宏亮并且清楚……”
- “这件事情告诉我……”
- “听起来不错。”

听觉主导感官的次感元范围如下：

- 音量（大/小）
- 音调（高/低声部）
- 音准（高/低）
- 节拍（快/慢）
- 距离（远/近）

在面对听觉思维者时，一定要注意自己的措辞。他们听到的词语表达将决定事情的成败。我见过因为用词不当而让会面效果从巅峰跌入低谷的遭遇，因为对方是听觉思维者。

3. 动觉

动觉思维者特别在意感受。他们能够记住事件给自己带来的感受：温暖的房间、拂过肌肤的清风、令他们惊恐而跳起的电影。动觉思维者通常会用自己的双手去感知物体。仅仅告诉他们某物柔软不如让他们触摸一下。但帮他们回忆曾经摸过的柔软的物体，可以让他们想起非常真实的情感和触感。

“动觉”这一词汇与触觉、本能以及身体的本体感觉有关，简单点说，就是身体在空间中所处的位置，以及事物让他感受到的自我意识。动觉思维者使用如下表述方式：

- “我能抓住那个想法的要点。”
- “那个是如何抓住你的？”
- “我会联系你的。”
- “我刚想联系来着。”

- “这感觉怎么样？”

动觉思维者的次感元范围如下：

- 强度（强/弱）
- 面积（大/小）
- 质地（粗糙/光滑）
- 温度（热/冷）
- 重量（重/轻）

帮助动觉思维者回想起与某一事物相关联的感觉或者情感，可以让那些情感再现。对于非动觉思维者来说，动觉思维者可能是最难应对的，因为他们对景象和声音都不会有反应。社会工程人员要想与他们沟通，得和他们进行感觉上的联系。

理解以上这些基本原则，能够帮助你快速辨别出对方是何种类型的思维者。再次回到原来的问题，在不询问对方早上起来的第一感觉的情况下，如何判断他的主导感官呢？就算判断出来又怎样呢？有那么重要吗？

4. 辨别目标的主导感官

想要确定对方的主导感官，首先尝试自我介绍，然后开始简短的交流，在此过程中留意对方所说的话。在你走向目标对象并和他打招呼时，也许他都没有正式地看着你。可能他比较无礼，也可能他不是一个视觉思维者。视觉思维者需要看着对方说话才能正确沟通，这种行为似乎证明他不是视觉思维者。这时，你可以再简单地问一句：“今天的天气让人感觉很舒服啊！是不？”观察他的反应，特别注意他是否会面露喜色。

也许你可以戴一个大的、闪亮的银戒指，谈话时不断地打手势，也许你会看到戒指引起了他的注意。他会不会感兴趣地伸手触摸，甚至想要拿在手里仔细看看？动觉思维者遇到这种东西会很想触摸。我认识一位女士，她是一个很明显的动觉思维者，每当看到自己认为质地柔软或高品质的东西时，她必须要摸一摸。她会说：“哇哦，那件毛衣看起来好柔软啊！”从这句话来看，我们可能认为她是视觉主导的，然而后面发生的事却证明了她是动觉思维者——她径直走过去，用手去摸毛衣、去感受。这个女人在去商店购物时必定会摸一下每件商品，不管她是否需要。通过触摸物体，她和商品之间建立了联系，这种联系让她觉得很真实。通常她对那些没有亲手碰触过的物品很难产生深刻的记忆。

用一些关键主导词来提问，观察目标的反应，然后认真地听他的回答，这样就能判断出他的主导感官。如果听到诸如看、瞧、亮及暗等字眼，可以表明目标是一位视觉思维者。当然，就像前文所述，这并不完全准确。并不存在一个通用规则。每一条线索都能够为你指明方向，从而据此提出更多的问题进行验证。友情提醒：如果使用与对方思维方式不同的模式进行交流，可能会让对方觉得不悦。不停地提问来确定一个人的思维模式，会令对方反感，因此在交流过程中，应

当注意尽量少问问题，多进行观察。

5. 为何了解思维模式如此重要

我曾和一位名叫托尼的人共事，他能够把水卖给将要淹死的人。托尼非常相信可以在销售工作中找出并利用对方的主导感官。他使用的一些方法值得我们借鉴。在第一次与目标人物会面时，他总是拿着那支很炫的、闪闪发光的钢笔，并打很多手势，观察目标的视线是否会跟随那支笔移动。如果有一点的话，托尼就会加大动作幅度，看他的目光是否会进一步跟随。如果在前几秒中未见成效，他会将笔帽不断开合，发出咔嗒声。声音不是很大，但足以干扰一个人的思绪。如果他是视觉思维者，就会引起他的注意。这招一旦奏效，托尼就会在对方每次认真思考时都这样“开合”一次，使得目标对这种声音和当时说的话产生心理上的反应。这招再行不通的时候，他会将手伸过桌面，轻拍对方的手腕或者手臂，或者如果坐得足够近的话，就会拍拍他的肩膀。当然他不会安排过多的这种肢体接触，他的目的是看目标人物的反应：是会害羞地躲开，比较乐意地接受，还是觉得自己被打扰了。

通过这些微妙的方法，他能够快速地判断出对象的主导感官最可能是哪一种。整个过程不会超过60秒。在发现期待的信息之后，他便会将后续的对话转移到主导感官领域，甚至通过谈话中的言辞、举止和响应体现出来。我见过的人当中，没有比托尼更会推销的了。认识他的人常说：“我感觉托尼很清楚地知道我的需求。”

托尼始终能够以目标人物自己喜欢的方式来愉快地聊天。如果目标是视觉思维者，托尼会用下述表述方式：“你看这个怎样？”他会使用一些诸如“看得见”的东西或者可视化的场景，令他们感觉处在一种非常舒适的氛围中。

人们在舒适的氛围中会备感放松。在社会工程过程中越是能将人们置于舒适的氛围，成功的几率就越高。人总是喜欢和让他感到舒适的同伴在一起，这是人的本性使然。举个例子，如果某人让你备感“温暖和贴心”，或者能够听懂你的话，或者能听出你的口音，你会轻易地信任他、向他敞开心扉，并允许他进入你的生活圈。

我想重申这个观点：识别并利用他人的主导感官并不是一门精密的科学。社会工程人员只能把它当做众多工具中的一种，不能完全依赖它，把它神化或者当成科学。某些人类本性方面的心理学知识是有一定科学依据的，具有一定的可靠性。事实上，其中有些会给人以深刻的印象，让你能够读懂别人的心思。有的在业界还存在一定的争议，有的则广为心理学家、执法部门和社会工程人员所认同。下一节会从微表情入手，就此进行深入探讨。

5.2 微表情

对于面部表情的解读，大家可能已经很熟悉了。人们的喜、怒、哀、乐等各种情绪都会通过

面部表情体现出来。如果有人使用虚假的表情呢，比如假笑？在集市上遇到不太喜欢的人时，我们会面带“微笑”地说：“约翰，真高兴在这里碰到你。替我向莎莉问好。”

我们可能表现得非常开心和兴奋，内心却很愤怒。面部那种长时间持续的表情叫做*宏表情*，一般情况下，这种面部表情更易于传达情绪。与微表情类似，宏表情也是由情绪控制的，但是并非自然流露，经常能够伪装。

几个研究人类行为的先驱花费了几十年的心血来研究并尝试理解人类是如何传达情感的，并最终将之命名为*微表情*。

微表情是情绪的自然反应，不大容易控制。情绪触发面部特定肌肉的反应，形成特定的面部表情。很多时候，这些表情的持续时间不过1/25秒。因为这些表情都是情感反应引发的无意识的肌肉运动，所以几乎不可能被人为控制。

这一定义也并不是首次提出的，1872年，查尔斯·达尔文在他的著作《人类和动物的情绪表达》（*The Expression of the Emotions in Man and Animals*）中提到过面部表情的通性和每种面部表情对应的肌肉运动。

20世纪60年代初期，两位研究员哈格德（Haggard）和艾萨克斯（Isaacs）最先发现了现在所称的“微表情”。1996年，他们在著作《面部微表情瞬间——心理的自我反应机制》（*Micromomentary Facial Expressions as Indicators of Ego Mechanisms in Psychotherapy*）中，阐明了发现“微瞬表情”的过程。

同样在20世纪60年代，人类行为学先驱威廉·康登（William Condon）花费了大量的时间，对长达几小时的磁带进行逐帧研究，发现了人类表情的“微运动”。他还在神经语言程序学（后期对此研究比较多）和肢体语言领域做过深入的研究。

或许微表情领域最具影响力的研究者之一就是保罗·艾克曼博士。作为先驱，艾克曼博士将微表情发展成今天的一门科学。他研究微表情40多年，获得了研究科学家奖，并于2009年登上《时代》杂志，成为年度最具影响力人物之一。

艾克曼博士和心理学家希尔文·汤姆金斯（Silvan Tomkins）一起研究面部表情，发现了与主流观点不同的研究成果：情感不是由文化决定的，而是在不同文化和物种间普遍存在的。

他和莫林·奥沙利文博士（Dr. Maureen O'Sullivan）策划出一个叫“巫师”的项目。他是将微表情运用于测谎方面的先驱，他们对15 000个来自各行各业的不同文化背景的人进行测试，发现在不经过专业训练的情况下能够躲过测谎仪的只有50人。

20世纪70年代，艾克曼博士开发出一套面部表情编码系统（Facial Action Coding System，缩写为FACS），用来对人类可能的表情进行标记和编码。这套系统不仅涵盖各种面部表情，还包括欺骗时整个身体的反应。

1972年，艾克曼博士将与最基本的、生物共有的情绪相关的表情列示了出来，包括：

- 愤怒
- 厌恶
- 恐惧
- 快乐
- 悲伤
- 惊讶

艾克曼博士的这些研究成果得到了推广，很多执法部门和企业开始应用他在测谎方面的成果。1990年，他在一篇名为“基本情绪”（Basic Emotions）的论文中对他之前的清单进行了修订，将情绪划分为积极的和消极的两种（详见www.paulekman.com/wp-content/uploads/2009/02/Basic-Emotions.pdf）。艾克曼博士还撰写了很多关于情绪、面部表情和测谎的书籍，帮助人们理解面部表情解码的价值。

从前面简短的介绍中不难看出，微表情并不是空穴来风。相反，它是人类行为学领域一代代博士、研究员、专家花费无数时间研究出来的成果。作为一名社会工程人员，懂得观察微表情可以有效地保护你的客户，教他们发现骗局中的微小漏洞。

如果你是一名社会工程人员，或者是对微表情感兴趣的人，我强烈建议你读一读艾克曼博士的书，特别是《情绪的解析》（*Emotions Revealed*）和《解密脸部：从脸部线索识别情绪的指导》（*Unmasking the Face*）。他是该领域真正的权威。接下来将对微表情进行简单的阐述，告诉你作为社会工程人员，如何将其运用到工作中。

前文提到艾克曼博士列出了6类主要的微表情，后来他又将“轻蔑”添加进来，变成了7类。下面将逐个进行介绍。

5.2.1 愤怒

愤怒和其他表情相比，通常是比较容易识别的。人在生气的时候会紧抿双唇、眉头紧锁，当然还有最为明显的特征：双眼圆瞪。

愤怒是一种比较强烈的情绪，它能够触发很多附带情绪。有时候当一个人对某件事情感到生气的时候，你会看到如图5-1所示的微表情。比较难以察觉的原因是这种面部运动可能只会持续1/25秒。

学会查看特定的微表情可以大大提升理解他人的能力。关于如何掌握这种能力，艾克曼博士建议大家自己做相应表情的练习，可以参考以下的步骤。

(1) 把眉毛往下拉，使其并拢到一块。仿佛是要使眉毛能够触碰到鼻子。

(2) 当眉毛下压的时候，尝试在眉毛不动的情况下，使劲睁大眼睛。

(3) 紧闭双唇。不要撅起来，只是让上下唇紧紧地抿在一起。

(4) 瞪眼。

该图片由保罗·艾克曼博士提供

图5-1　注意瞪圆的双眼、紧抿的嘴唇和紧锁的眉毛

你感受到什么样的情绪？我第一次尝试的时候，感到异常愤怒。接下来提到的是本章的要点。

> 如果制造出面部表情可以引发一种情绪，那肯定意味着面部移动可以影响我们感受到的情绪，甚至可能感染周边的人。

对着镜子持续练习这种表情，直到做对为止。图5-2所示的就是西蒙·考威尔（Simon Cowell）展示出来的一种非常典型的愤怒表情。

该图看起来可能没有图5-1那么明显，但是从他的脸上可以识别出与愤怒相关的所有微表情。

拥有熟练掌控微表情的能力对有效理解这些表情背后的情绪十分有用。当能够成功做出并解码微表情，你便能够理解引发这种表情的情绪。这样你就能够明白对象的精神状态。不仅要能够

做出各种微表情，还要主动解读周边人物的表情，这会对你控制社会工程活动的成果大有裨益。

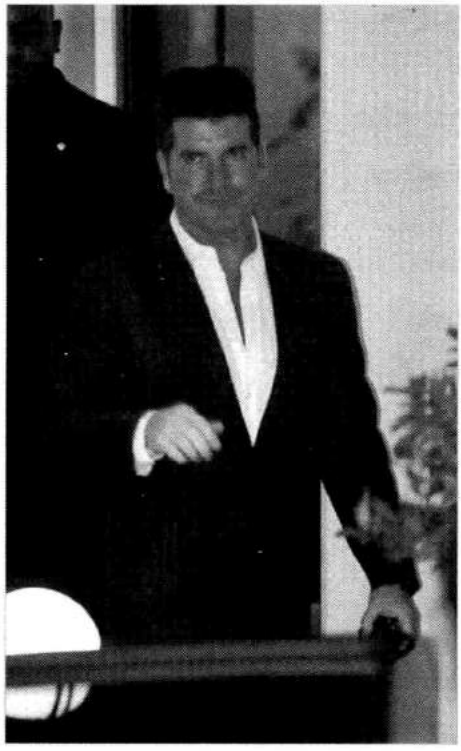


图5-2 西蒙绝对是愤怒了，注意他的表情

5.2.2 厌恶

厌恶通常是对你确实不喜欢的东西产生的一种强烈的反应。这种“东西”不仅限于物理实体，有的时候也可能是一种信念或者感觉。

极为讨厌的食物会令你产生厌恶的感觉，就会触发这种微表情。不可思议的是，即便在没有闻到或看到这种食物的时候，想到它都会引发同样的厌恶情绪。

十几岁的时候，我和几个朋友一起去迪士尼乐园。我当时并不喜欢也不想去玩过山车，然而最终还是招架不住朋友的劝说，去了太空山——一个室内过山车项目。快到一半时，还觉得过山车对我来说其实也没什么，但突然发现身上沾了一些湿湿的恶心的东西，然后就是一股恶心的气味令我作呕。不仅是我，身后的很多人也有类似的反应，可以说基本上没有人能忍住不吐。很快地，大家几乎同时呕吐在了另一辆“未来世界”列车的车窗玻璃上，该项目是为了让游客在行驶缓慢的列车上体验太空山之旅。让我们吃惊的是，乘坐“未来世界”列车缓慢在园中游览的旅客看到车窗上的呕吐物时，竟然也开始呕吐了，尽管他们并未闻到或接触到窗体外

我们的呕吐物。这是为何？

厌恶。体液通常会让人产生厌恶的感觉，这也是你读上文时可能已经开始觉得厌恶的原因之一。

厌恶通常表现为上唇上启、露出牙齿，鼻子皱成一团。有时随着鼻子皱起，双颊会上移，感觉想阻隔难闻的气体进入鼻腔或者阻断恶心的想法进入自己的私人空间。

有一次我在看一篇关于冬奥会的文章，一张叶卡捷琳娜·尤金娜（如图5-3所示）的照片就清晰地显现出厌恶的特征。注意观察她那上抬的嘴唇和皱起的鼻子。她是在看自己的得分吗？被对手打败了？我不确定，但她正在看的东西一定令她感到不快。

图5-3　皱起的鼻子和上启的嘴唇是厌恶的明显表征

根据艾克曼博士的研究，厌恶是一种情绪，它是肌体对于看起来、闻起来甚至想起来觉得恶心的事物的一种反应。从社会工程的角度来看，这种情绪可能会导致失败，然而这些反应可以帮助你判断自己是否已达到目的或者是否已经引起目标的反感和排斥。

一般情况下，不论是什么原因导致你的目标产生了这种表情，都宣告了你的失败。如果你的外表、体味、风格、气息或者其他方面让他人感到厌恶，那么大多数情况下你已经失败了。你必须意识到目标的好恶。例如，如果审计的对象是一个知名的律师事务所，而你身上有很多穿刺或纹身，就会给目标带来强烈的反感，这可能直接将你的社会工程行动扼杀于摇篮。当你看到如图5-4所示的表情时，就要做好离开的准备了。

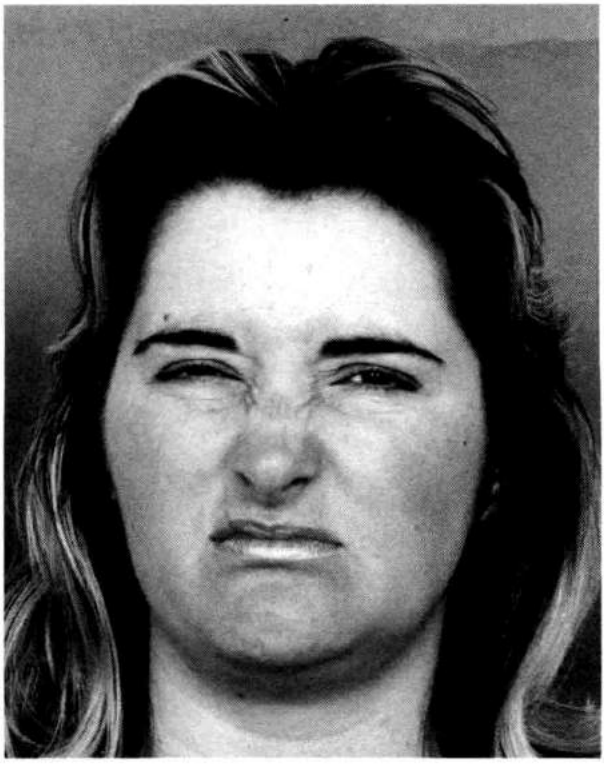


图5-4 如果看到这种表情，就说明有问题了

在伪装时，必须认真考虑你的外表。一旦发现目标脸上出现厌恶这种强烈的负面情绪，较好的方式是赶紧放弃，礼貌地为自己开脱后，考虑一种新的伪装或者另辟蹊径。

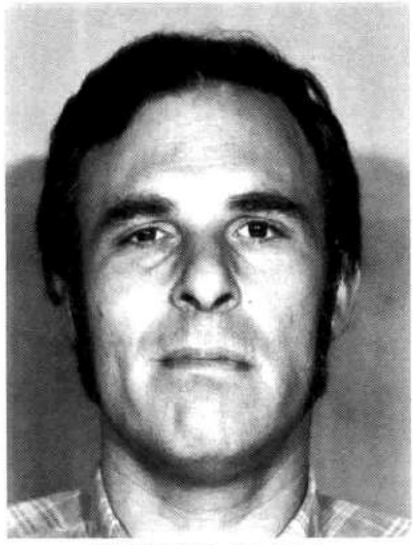
5.2.3 轻蔑

轻蔑是一种很强烈的情绪，通常会与厌恶混淆，因为两者具有紧密的关联。艾克曼博士甚至在起初的基本情绪列表中没有写上轻蔑。

在艾克曼博士的《情绪的解析》一书中，他做过如下描述："轻蔑只是针对人或者人的行为，而不是针对味觉、嗅觉或者触觉。"他举了个吃牛脑的例子，你可能会因为这种想法而觉得恶心，这就会引起厌恶。而看到正在吃牛脑的人时，就会触发"蔑视"，不是对这种行为，而是针对吃牛脑的那个人。

在我看来，这一点非常重要，理解该微表情也很重要。蔑视通常针对的是人，而不是具体的物体，这对我们理解这种微表情所表达的含义非常重要。如果能够看出目标对象是否带有轻蔑的表情，就能帮助我们更清晰地找出他产生这种情绪的真正原因。

轻蔑的表情一般伴随着皱起的鼻子和上启的上唇，但只会出现在脸的一侧，而在厌恶的表情中，整个鼻子都会皱起，整个上嘴唇都会上启。从图5-5中就能看出一丝细微的轻蔑表情。



该图片由保罗·艾克曼提供

图5-5　请注意观察艾克曼博士的脸——微皱的鼻子和上移的右脸

尝试模仿“轻蔑”的表情。如果你像我一样，过不了多久就会感到心中产生的愤怒和轻蔑的情绪。做这种模仿练习，并且观察这种模仿给情绪带来的影响是件有趣的事情。

在图5-6中，小威廉姆斯（Serena Williams）明显表现出了轻蔑的特征。我从网上找到的这张图片，但是没有将整篇新闻稿保存下来，因此并不知道她轻蔑的对象是什么。但是不管是什么，她明显对其感到不爽。

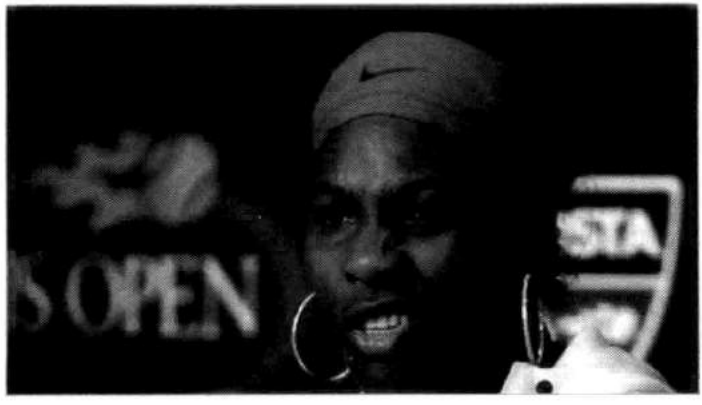


图5-6　小威廉姆斯的左脸表现出了轻蔑

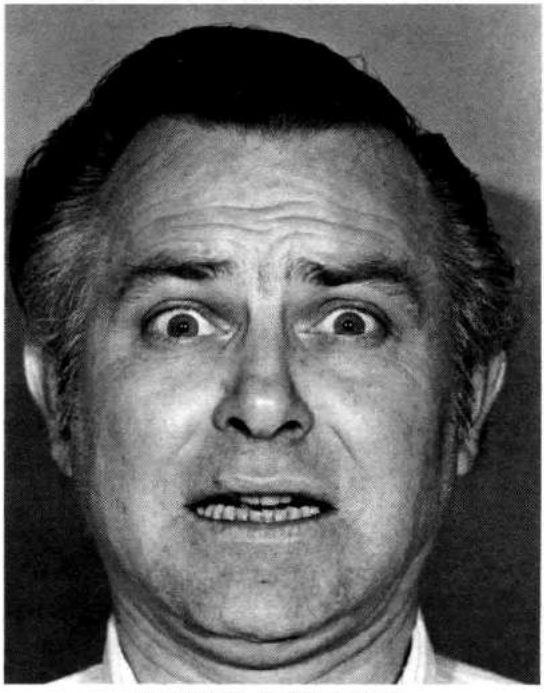
让人们产生轻蔑情绪的事情也会触发强烈的负面情绪，因此轻蔑通常会伴随着愤怒。轻蔑是和他人打交道时要尽量避免的情绪，尤其是在社会工程过程中。

5.2.4 恐惧

人们经常混淆恐惧和惊讶，因为这两种情绪引起的面部肌肉运动非常相似。最近在飞机上，我正准备写“快乐”那节，但当时发生了些意想不到的事情，直接导致我撰写了“恐惧”这节。

我身高6英尺3英寸（约1.9米），不矮也不瘦。坐在飞机上，想到还有几个小时要打发时，我决定利用这段时间来工作。这里我要插一句，当时的经济舱座位有些不同。我坐下后，打开笔记本电脑，看着外面的天空，开始思考如何撰写“快乐”一节的开头。不一会儿，我就决定写“恐惧”，因为旁边的乘客拿出一瓶水喝了一大口，但没盖上瓶盖。我用眼角的余光看到瓶子从他手中滑落，倒向我的键盘。我当时的第一反应就是“恐惧”。

我瞪大双眼，皱起眉毛，嘴唇同时向耳朵拉起。当然，事发当时，我并没有意识到这一切的面部变化，但是后来在对发生的事情进行回想和分析时，我知道自己当时感到的是恐惧。我分析了自己当时面部肌肉的移动方式，得以确定如果我不断重复这样的表情，会体会到相同的情绪。我确定自己当时的表情和图5-7所示的表情类似。



该图由保罗·艾克曼博士提供

图5-7 恐惧的明显特征

请尝试以下步骤，看你能否产生同样的情绪。

(1) 使劲往上抬眉毛。
(2) 缓缓张开嘴巴，向后咧开嘴角。
(3) 如果可以的话，在眉毛上扬的过程中努力使它们皱在一起。

感觉如何？你的双手、手臂还有胃有什么感觉？是不是感到有点害怕？如果还没有，再试一遍，只是这次尝试去想象一个你控制不了的情景（类似我在飞机上的那段经历，或者是伴随着轮胎尖锐的摩擦声，前方车辆紧急刹车）。这时感觉怎么样呢？

通常情况下，你会感到害怕。我从网上找到一张带有明显恐惧特征的照片（参见图5-8），照片里的人是美国参议员奥林匹亚·斯诺（Olympia Snowe）。暂不管拍下该表情之前她被问了什么问题，她的恐惧表情从照片中一眼就能辨别出来。她的眉头高高抬起，双唇向后微张，而且上扬的眉毛几乎皱到了一起。

图5-8　斯诺参议员明显的恐惧表情

从一名社会工程人员的角度来看，恐惧经常被用来诱使目标对象做特定的反应和动作。具有恶意动机的社会工程人员通常会对毫无戒备心的用户运用这种伎俩，从而诱使他们点击特定的图标或者泄露有价值的信息。例如，有些恶意的提示词如下："你的电脑感染了病毒，点击这里进行修复!!"这些标语对于不懂技术的人百试不爽，他们会由于担心中毒而点击进去，结果电脑就真的感染了病毒。

我曾经合作过的一家公司就被一名心怀恶意的社会工程人员攻入了，他当时利用的就是员工的恐惧心理。在得知公司的CFO出城参加一个重要的商务会议，期间不便被打扰后，该社会工程人员伪装成一名技术支持人员混进了公司。他要求进入CFO的办公室，但被拒绝了。然后他使用了如下伎俩："你们的CFO史密斯先生打电话给我，叫我在他出席会议的这段时间帮他把电子邮箱的问题处理好，如果在他回来之前解决不了，后果会很严重。"

秘书担心如果不把CFO的电子邮箱问题解决，自己会受责罚。她的老板会不会大发雷霆？她

会不会因此丢掉工作？鉴于对不良后果的担忧和畏惧，秘书让这位“技术支持人员”进去了。如果该社会工程人员经验丰富，他可能就是通过观察秘书的面部表情得知了她的心理动态，通过不断强化她的担忧和紧张，使她达到恐惧的状态，从而实现自己的目的。

恐惧是一种强大的推进器，可以使你或者目标对象做出异于平常的事情。

5.2.5 惊讶

如前文所述，艾克曼博士和微表情领域的其他心理学家认为惊讶和恐惧有着密切的联系，因为从表情上来看二者存在很多相似的地方。尽管如此，二者还是有些明显的不同，例如嘴唇移动的方向和眼睛反应的方式。

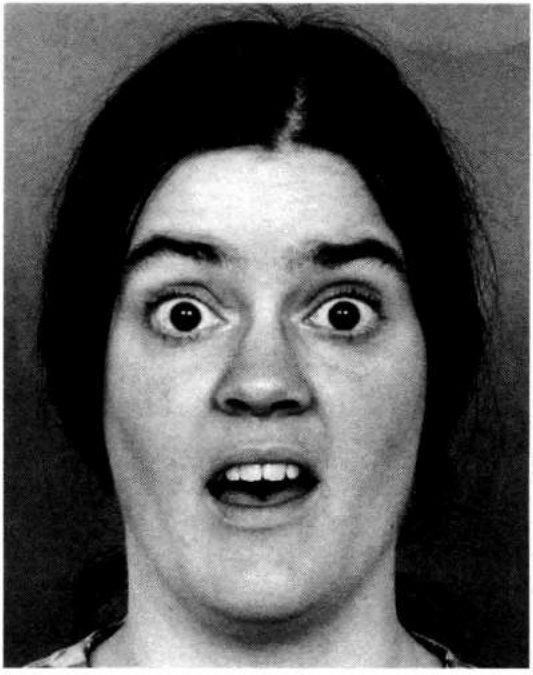
请试着做以下动作来练习“惊讶”。

(1) 抬起眉毛，不是充满恐惧而是抱着想尽量睁大眼睛的目的去做。

(2) 轻轻地张开下颚。

(3) 练熟这个表情以后，试着加快速度。

我注意到自己做这种动作的时候不经意间吸了不少空气，这让我感到一种类似于惊讶的情绪。你应该会看到类似于图5-9所示的表情。



该图由保罗·艾克曼博士提供

图5-9 注意眼睛和双唇是不是与恐惧的表情类似

令人感到惊讶的可能是好事情，也有可能是不好的消息。听到女儿牙牙学语时蹦出的字眼当然是件令人吃惊的好事情。某些意料之外的事情、通知或者问题也可能导致惊讶的反应。

这便是我对于图5-10中杰西卡·辛普森（Jessica Simpson）的表情所传达的内容的猜想。注意观察她上扬的眉毛和张开的下颚。她表现出来的惊讶特征较为明显，可能刚被问到了一个令她感到吃惊的问题，或者是听到了什么震惊的消息。

图5-10　除了一些细微的差别，惊讶经常会被误认为是恐惧

如果是积极的惊讶，通常会引发一丝微笑或快乐的表情。如图5-10所示，从杰西卡的表情不难看出，她不仅是惊讶，而且还带有一丝惊喜在其中。社会工程人员有时会利用惊讶来打开目标对象的心门，比方说，机智的对答或不经意间的玩笑可能会使目标马上放松警惕，降低其心理防线。

5.2.6　悲伤

悲伤是一种强烈而极端的情感。我们看到他人悲伤，很容易心生怜悯，感同身受。有些人看到别人悲伤，自己就会产生悲伤的情绪，甚至也会哭泣。

通过以下练习，很容易产生悲伤的感觉。

(1) 轻轻地张开嘴巴。
(2) 下咧嘴角。
(3) 保持嘴唇不动，同时上抬你的双颊，感觉自己眯着眼睛。
(4) 保持表情不动，眼睛往下看，让上眼睑无力地下垂。

通常这个时候，你便会产生悲伤的情绪了。我第一次做这个表情的时候，就立刻奏效了。我发现自己得控制练习这个表情的时长，因为练习带来的悲伤会持续较长的一段时间。图5-11展示的便是“悲伤”的表情。

DR. PAUL EKMAN对应：该图片由保罗·艾克曼博士提供

图5-11 注意双唇和下垂的眼睑，这意味着悲伤

悲伤的另一个特征使它成为一个奇妙的情感，即它并不需要显现出极度的痛苦或悲伤。悲伤可以表现得非常微妙，可以用局部的面部表情来传达。人们可能会试图使用虚假的微笑或者“坚忍的眼神”隐藏悲伤——凝视正前方，面容呆滞，但你可以看出他们正试图控制内心的真实感觉。

请看图5-12，图中展现的就是这种表达方式的悲伤。在对凯特·戈瑟兰（Kate Gosselin）的

一次有关离婚和家庭的采访中，她极力地隐藏自己内心的情绪，然而如果仔细观察她的双唇，你就会发现一些细节之处体现了她内心的悲伤。

图5-12　注意双唇咧向后下方，这意味着悲伤

除了双唇，眼睛是传递悲伤的另一个关键信号源。这种表情有时难以发现，甚至会被误认为是疲劳或者其他情绪，不过通过观察他的行为举止和肢体语言可以找到一些线索。

遮住大部分脸的这种文化充分体现了这一点。如图5-13所示，一群妇女参加葬礼，尽管她们的大部分脸被头巾包住了，但中间那位女子眼神中流露出的悲伤清晰可见。

营造悲伤的气氛也是社会工程常用的手段之一，因为它可以激发人们采取某些行动，从而捐款或者提供信息。类似桥段经常出现在电视里的商业广告中：一些无助的孩子，他们缺少爱和关怀，长期生活在清贫的环境里，营养不良，只要你献出一点爱心，就会让他们的脸上浮现笑容。悲伤的神情、满是泪水的脸庞，这些瘦弱的儿童始终会扣紧你的心弦。我说这些并不是意味着商业广告是恶意的社会工程，只是想说明它们使用了一定程度的社会工程，通过触发情绪让目标做出特定反应。

不过恶意的社会工程人员通常会利用人们这种同情心从目标那里获取利益。有一次我走进一家餐馆，无意间听到一位年轻的男子和一群准备走出餐馆的长者的对话。据他描述，他刚从高速下来，车子没油了，他现在急需赶往家中，因为家里的妻子有着9个月的身孕。他刚失业，徒步从高速公路走了一英里过来这边给妻子打电话，他想找这些被他拦住的人借20美元。我听到一半便放慢脚步，装作在打电话，等着看接下来的戏。他继续说着故事，最后加上一句："你把地址给我，我到家便会把20美元的支票寄还给你的，我发誓！"

图5-13 注意她下视的眼神和下垂的上眼睑

这个故事具备了引发他人同情的要素，尤其当他脸上流露出那种对家人的担忧、焦虑和悲伤时。他得到的何止20美元，那三位长者一人给了他20美元。他说了几遍“愿上帝保佑你们”并逐一拥抱了他们，然后说自己进去就打电话给妻子，告知她自己在回去的路上。拥抱后，他们几个就离开了餐厅，心里美滋滋地觉得自己这周又做了一件善事。

几分钟后我在用餐时，发现那个年轻人在吧台和同伴享用各种酒水饮料呢。他能够很好地操控周围人的情绪，将悲伤的故事结合悲痛的表情演绎了出来。

5.2.7 快乐

快乐有很多方面，估计单单快乐这一话题就可以讲一章，然而这并不是我关注的。艾克曼博士的书中有很多关于快乐和相近情绪的绝妙观点，里面阐述了这些情绪如何影响自己及身边的其他人。

我在这里想强调的只是快乐的几个方面，最重要的一点便是如何辨别微笑的真伪。识别真假笑容是帮助我们更好地读懂人类表情的重要方面，对社会工程人员来说，这有利于他们掌握如何呈现笑容。

你有没有过这种经历：碰到某个人，他看起来很开心，但是在和他辞别后，你的配偶或者你自己会觉得刚刚这人笑得好假？

你可能并不清楚什么样的笑容才称得上真实，然而脑子里总有种声音告诉你“这家伙在假笑”。18世纪晚期，法国神经学家杜兴·德·布伦（Duchenne de Boulogne）针对笑容做过

一些卓有成效的研究。他将电极附着在试验者的脸上，通过电流产生和微笑一样的肌肉反应。尽管试验者的肌肉和正常微笑时的运动完全一致，德·布伦还是觉得他是在“假笑”。这又是何故呢？

德·布伦指出，当一个人真实地微笑时，会触发颧大肌和眼轮匝肌（眼周的肌肉）两块肌肉，而眼轮匝肌的运动是自发的，不受外力触发，这也就是辨别真假笑容的关键所在。

艾克曼博士与杜兴的研究成果不谋而合。虽然近期的研究表明有些人可以通过训练来触发那块肌肉，但通常情况下，真假的辨明就在于眼睛。真实的笑容是由眯着的眼睛、上扬的双颊和拉起的下眼睑构成的。它由眼及口，牵扯到整个脸部的运动，如图5-14所示。

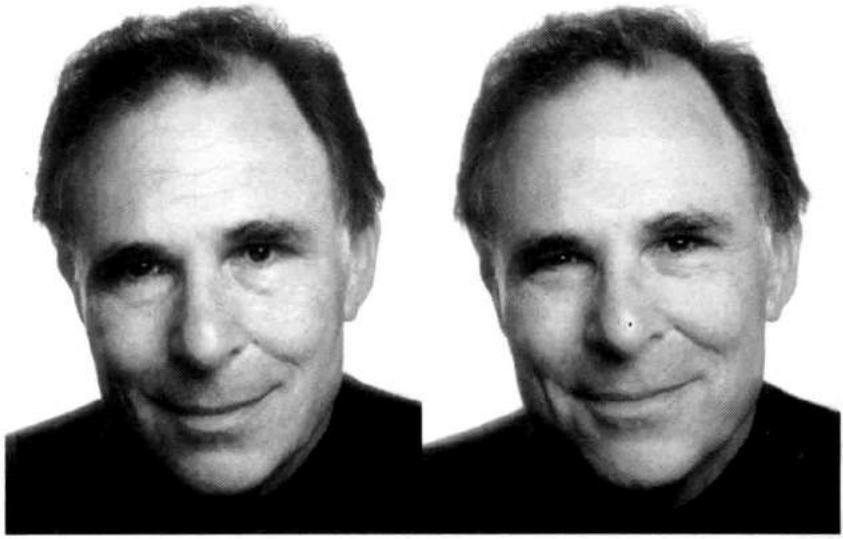


图5-14　艾克曼博士演示的假笑（左图）和真笑（右图）

如果你遮住艾克曼博士的上半部分脸，估计会很难区分笑容的真假。直到看到左右两图中艾克曼博士眼睛的对比，才能区分得出来。

如果一个人对他人展示出发自内心的笑容，在他的感染下其他人也会流露出相同的喜悦并微笑的。注意图5-15中的两个和尚，左边那个和尚展现出了真实的笑容，他是真的开心。你看着图片中的他，自己也会跟着开心起来。

从社会工程的角度来看，知道如何觉察和伪造出以假乱真的笑容是很有价值的。他们竭力想让目标对象放松，从而得到最积极的效果。不管伪装成什么角色（销售人员、教师、心理学家或其他的角色），社会工程人员开启对话的第一步通常是一个微笑。我们的大脑在接收到这个视觉输入后会快速地进行分析并得出结论，对这个微笑真伪的判断直接影响后续的交流。

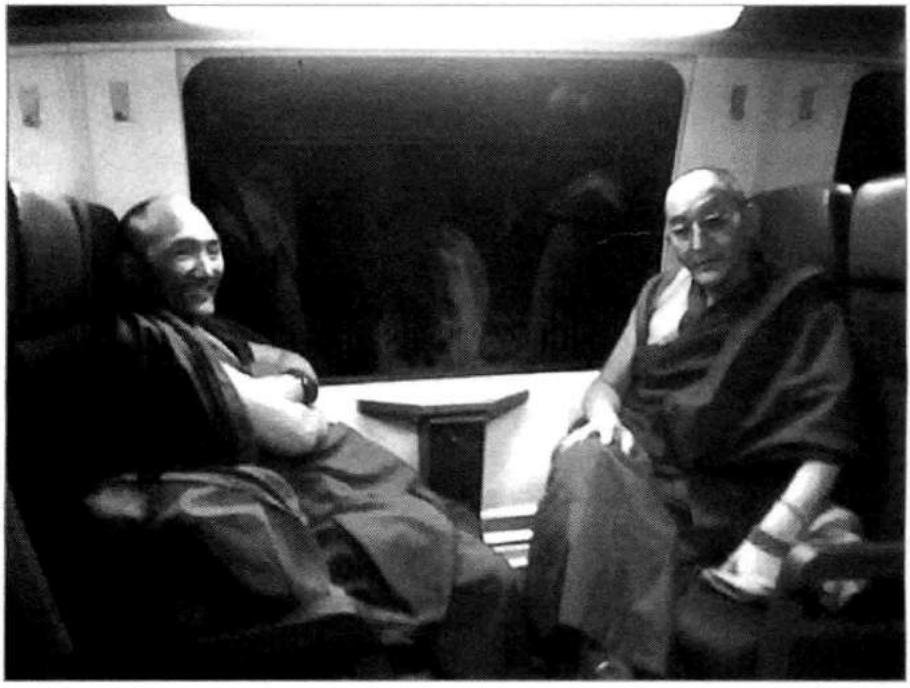


图5-15 他整张脸都在笑

前文涵盖了很多信息，你可能想知道社会工程人员是如何训练自己，从而不仅能够识别微表情，还能够熟练地运用的。

5.2.8 训练自己识别微表情

好莱坞经常会夸大影视剧中角色的能力。例如在热播的电视剧《别对我说谎》（*Lie To Me*）（基于艾克曼博士的研究）中，剧中的主角莱特曼博士（Dr. Lightman）可以毫不费力地读懂他人的微表情，更神奇的是他通常能说出情绪产生的原因。

然而在现实生活中，这一领域中，像艾克曼博士这样的人员所做的大部分工作并非这么轻松，这种研究意味着坐在录好的视频片段前逐帧地进行分析。这样的研究要做好多年，他才能快速注意、识别和分析微表情。20世纪70年代，通过一项专题研究，艾克曼博士发现有些人天生就具有感知并准确分析微表情的能力。

然而具备这种能力的人毕竟是极少数，所以大部分人都需要不断地练习及训练，才能够熟练地展现、读懂并运用微表情。在这里和大家分享一下我的训练方法。我先研究特定微表情的鉴别方法，然后对着镜子参照专家描述的步骤进行模仿。通常我都会拿一张展示这种情绪的照片，对着照片模仿对我大有帮助。

当觉得自己模仿得不错的时候，我便开始专注于酝酿感情、调整细节，直至面部肌肉的运动和情绪能够一致。

然后，我从网上寻找不同的表情图片，试着去揣摩其表达的情绪。接下来试着将新闻或电视节目录下来，以较慢的速度去静音播放，看自己能否准确辨别说话者的情绪，之后再听原版的故事，看自己猜得是否接近原意。这些都是为“实战”做准备。然后我会观察人们之间的交流，尝试识别他们交谈过程中的情绪波动。我不仅会观察那种可以听到谈话内容的对话，也会观察那些无法听到交谈内容的场景。

我之所以没有直接在自己的会话中练习，是因为不用在训练的时候去注意自己的谈吐和话题的接转，这样要更容易些。我只需专注地去阅读面部表情即可，不用被自己其他的感觉所干扰。在有幸见到艾克曼博士之前，我一直是按前文所述的这种方法训练的，见到他之后，他传授给我另外一套方法。当然，还有他的那些著作，里面有解读和重构表情的分步式的教学方式，还有不同情绪所对应表情的照片、新闻中的实际例图等。他的《情绪的解析》以非常专业的方式对此进行了解读，该书非常值得一读。

近几年，艾克曼博士研究并发布了针对微表情的专业训练。在网站www.paulekman.com中，他提供了3种训练模式，从而改变了人们掌握这门强大科学的方式。

针对每一种微表情，艾克曼博士的训练课程都有视频和文本说明。网站用户可以重放每一种表情的形成过程的视频，观察面部运动的每一个细节。一旦学员花了足够多的时间在上面学习并观察这些视频，便可以参加预备测验，检测自己对于微表情的识别达到了何种水平。当学员提交自己的猜测结果后，正确的回答会得到确认，错误的回答会得到纠正。如果需要纠错的话，可以参加额外的学习和培训。

当用户觉得胸有成竹的时候，可以参加正式的测试。最后的考试没有纠错，学员将要辨别时长为1/25秒的微表情，然后必须作出判断，到最后才有总分。

根据学习的成长（效果）曲线，通过这种训练工具训练几年，就能熟练解读微表情了。然而，艾克曼博士和他的同事却警告说：就算你精于解读微表情，仅能解读它也是远远不够的。他们何出此言呢?

演员常用的一种技巧是尝试从过去的记忆和经历中成功找到和想要表达的情绪一样的事件，例如回忆过去的一个快乐瞬间就会产生一个真实的笑容。前文曾提到，如果并不开心，想要刻意装成很开心是很困难的，但是如果你能唤起让自己感到开心的回忆，你的面部肌肉便会依据记忆作出自然的反应。

因此，尽管可以熟练地辨别微表情背后的情绪，却很难读懂每种情绪的触发因子。这种因子无法从科学的角度去阐释。我有一个朋友，在儿时曾经与某人有过一些不愉快的经历，而那个人和我的另外一个好朋友长得非常像。每当我这个朋友来访，她的情绪都会有很大的波动。你可以

从她面部的微表情中读到恐惧、轻蔑和愤怒。她并不是讨厌我那个朋友，而是讨厌那个记忆深处长得和我朋友很像的那个人。

在学习解读微表情时，记住下面这一点很重要。每种表情背后都有一种情绪，然而仅仅通过表情是无从得知该情绪的起因的。当学习微表情达到比较“熟练”的地步时，我感觉自己就像掌握了读心术一般。事实上一定要当心，不要想当然，离“读心”还远着呢。也许你已经精通读懂微表情的方法了，接下来便教你如何把这种技巧与沟通手段、肢体语言以及诱导方式有效地结合起来运用，让你不仅能够明确目标对象的想法，还能够将他们引到你想要的方向。

可能你心中还有一个疑问：“作为社会工程人员，要怎样运用这些技巧呢？”

5.2.9 社会工程人员如何运用微表情

研究很让人着迷，背后的心理学原理很神奇，但我们如何将微表情应用于社会工程审计呢？恶意的社会工程人员会怎么利用它呢？本小节就是要给出该问题的解答。

本节将讨论两种将微表情运用于社会工程的方法。第一种是使用微表情去诱导或者诱发某种情绪，第二种则是使用微表情识别欺骗。

首先来看第一种方法，使用微表情令目标对象产生相应的情绪反应。近期读过的一篇研究论文改变了我对微表情的认识，令我见识了一个新的研究领域。研究人员李文（Wen Li）、理查德·津巴（Richard E. Zinbarg）、史蒂芬·勃姆（Stephan G. Boehm）和肯·派勒（Ken A. Paller）发起了一项名为“情绪在下意识里的面部表现和性格焦虑带来的影响在神经和行为上的证据”的研究，这项研究改变了微表情在当代科学中的应用。

研究人员在试验者的面部肌肉上连接了几十个迷你心电记录器。这些器件将试验者脸上和头部肌肉的运动记录下来。然后，他们为试验者播放多段视频，视频中包括1/25秒时长、一闪而过的微表情。李文等人发现，几乎在所有情况下，试验者的肌肉运动会重复视频中嵌入的微表情。如果是恐惧或者悲伤，试验者的面部肌肉会产生相应的情绪。问及试验者的感受时，他们表示和视频中嵌入的情绪是一致的。

对我来说，这项开创性的试验表明，人们可以通过一些情绪上的微妙暗示操纵他人达到特定的情绪状态。我从安全角度开始了这方面的研究，并称之为“神经语言入侵”，主要原因在于它将微表情与神经语言程序学（下一节讨论）结合起来，在目标心中产生某种情绪状态。

设想这样的场景：一名社会工程人员要进入一家公司，目的是让前台将带有恶意程序的U盘插入电脑。他的伪装是和人力资源经理约好了过来面试，但路上不小心将咖啡洒到最后一份简历上了。他真的需要这份工作，也需要前台的帮助。前台会帮他重新打印一份简历吗？

这一伪装在引起对方共鸣方面相当有效，我之前就利用它获得过成功。然而，如果社会工程

人员不能很好地控制自己的情绪，就可能会表现出恐惧，从而引发紧张。这种恐惧可能会转化为前台人员的紧张，最终导致自己的请求被拒或者行动失败。而如果他能够控制好自己的情绪，让自己表现出微妙的伤心的微表情，就会轻易激起同情，而他的请求也就很容易获得应允。

回顾前面讨论的广告，它鼓励市民“每天捐赠一美元，养活一名贫困儿童”。在要求捐款之前，在显示电话号码和网址之前，在告诉你接受信用卡捐助之前，电视屏幕上会展示很多伤心孩子的照片。这些亟需救助的痛苦的孩子的照片会引发你的怜悯，促使你做出捐助的行为。

这些广告对每个人都奏效吗？当然不是。然而，虽然不是每个人都捐，但它会影响几乎所有人的情绪状态。这也是社会工程人员充分使用微表情的方式。学习展现这些带有暗示性的微表情，会引起目标对象大脑中的神经元反映相同的情绪状态，使他更愿意遵照你的要求去行动。

这种微表情使用方式也被用于恶意的目的，所以我想花点时间谈论如何防御这种攻击（第9章也会介绍这方面内容）。要注意微表情的使用方式，但这并不意味着需要将公司里的每个人都培训成微表情专家。其真正的含义是必须加强良好的安全意识培训。即使对方设计出来的请求让你很有欲望去帮助、拯救或照顾，也要确保首先贯彻安全策略。可以简单地说一句：“对不起，我们的电脑不允许接入外来U盘。不过，离这里两英里处有一家联邦快递金考快印店。你可以去那里重新打印简历。需要我告诉史密斯女士你会晚到几分钟吗？”

在这种情况下，如此的婉言拒绝不仅能够让社会工程人员的计划泡汤，也会让目标觉得自己帮助了他人。

想要发挥微表情的作用，有时也需要和人类行为的其他方面相结合。第二种方法——识别欺骗，将会告诉你如何做到这一点。作为社会工程，使用微表情的第二个方法的目的在于识破骗局。如果你可以通过问一个问题，知道他人的回答是否真实，会不会感觉很好？这也是专家们热烈讨论的话题，有些专家认为通过眼神、肢体语言、面部表情或结合以上3点就可以识别真伪。然而有些专家却不以为然，还有一些专家认为这可以作为一门精准的科学来应用。

尽管各方的观点都有一定的事实论据，但是如何运用微表情来识别骗局呢？

要回答这个问题，思维就不能被微表情所局限，因为通贯本节的内容，微表情都是以情绪和情绪的各种反应为基础的。因此阅读本节时请铭记这一点，本节还分析了一些因果关系。

以下4种反应可以帮助你识别目标的诡计。

- 矛盾
- 犹豫
- 行为的变化
- 手势

下面将详细地讨论这些反应。

1. 矛盾

“矛盾”这种情况处理起来特别棘手，因为它们可能确实会在现实中发生。我就经常会忘记一些事情的细节，而我的妻子总会迅速地予以补充。在得到一些提示之后，我通常就能记起完整的故事。这并不意味着我在故事或对话的一开始就撒谎，而是在一开始就整件事发表评论的时候，我并不能记清每个细节，或者是我认为自己记得，而实际上并不记得。即便我“想起”了具体细节，也不是实际发生的情况，而可能是我自己认为的事实。

在评估是否将矛盾作为说谎的线索时，对这种无意的“谎言”进行考虑显得尤为重要。一旦发现矛盾的情况，你所要做的应该是挖掘更多的信息。就矛盾之处进行询问，注意观察他的微表情变化，也有助于对真实情况作出判断。

例如，假设你伪装成上门拜访的销售人员，打算通过给他们的CEO派发特价CD的方式进入公司内部。你事先了解到这位CEO比较关注某慈善机构，所以伪装的角色与此有关。当你走进大堂时，前台接待却说：“对不起，他不在，你把东西留在我这里就可以了。”

你知道如果就这样将CD留给她，那么其中植入的恶意程序很可能永远不会发挥作用。而且你觉得他在公司，因为看到他的车就在停车场，而且今天是工作日。综合这些事实，又不希望前台难堪，你说道：“哦，他不在吗？我前几天给他打电话询问什么时候可以过来拜访，他说今天可以。我记错日子了吗？”

如果你出对了牌且表情真诚，可能会有以下两种结果。

- 她可能会镇定地告诉你说：“对不起，他不在公司。”
- 她可能会前后矛盾（这可能是她之前没有说实话的一个线索）：“让我再确认一下。”

什么？她从坚决地声称“他不在公司”转成“让我确认一下”。这一前后矛盾足以提醒你应该挖掘更多的信息。她说这句话时有哪些微表情？她有没有因为撒谎而感到羞耻或难过？她有因谎言被拆穿而生气吗？她为所犯的错误感到尴尬或困惑吗？你不能想当然地断定她在撒谎，因为也许她是真的不知道，在你辩驳的时候她才决定去确认清楚。

在她核实之后，必要的话可以挖得更深一些，探查更多信息，以试探事实真相。你可以重申：“可能是我记错日子了。”通过仔细观察她的面部表情能够精准地判定她是否在撒谎。

第一轮交谈下来，如果你在她脸上看到了愤怒的特征，继续刨根问底可能会使她更加愤怒和尴尬，导致会话的终止。这时候，你可能要这样问：“如果史密斯先生现在不在，可能真是我记错会面的时间了，那么什么时间过来能见到他呢？什么时间最合适？”

这种类型的问题可以令她挽回面子，还给了你解读她面部表情的另一次机会。如果你注意到她的脸上并没有流露出愤怒，而是有点难过或者尴尬，你可以回之以同情和理解，让她能够敞开心扉。“我敢发誓，他和我约好今天见面。可是我的记性很差，我老婆甚至说我有老年痴呆症。

我买了部智能手机，如果知道怎么设定的话，可能会对我的记忆有所帮助。我也不想添麻烦，只是我什么时候能过来把东西给他呢？我一定得亲自交到他手上。”

留心观察细小的矛盾之处，因为它们可能是欺骗的关键标识，能够帮你迈进门槛。

2. 犹豫

和矛盾类似，你也可以通过他人的犹豫识别潜在的谎言。如果你问一个他本应即刻回答的问题，而他却犹豫不决，可能是他在利用迟疑的这段时间来编造答案。

例如，当妻子问我新买的电子设备多少钱时，她知道我肯定记得。如果此时犹豫的话，往往意味着我在盘算是否要如实回答，当然也有可能我确实在回忆价格。

当从学校提供的成长报告中发现儿子有X天缺席，而我印象中只有2~3天时，我问他其余那些天是怎么回事。如果他的回答是：“爸爸，还记得有一次我们预约了医生看病，然后你让我在家休息一天，还帮着你一起做项目吗？”这很有可能是实话，因为他反应够快，并且有事实作为支撑。不过，如果他犹豫了一下说：“哦，我不知道，可能报告搞错了。”此时要注意观察他说这句话时的微表情。是因为被抓而觉得愤怒？还是为想象的惩罚感到难过？无论是哪种，我都应该深入调查那些天他到底在哪里。

另一种需要注意的众所周知的犹豫战术就是重复你所提出的问题，好像是对问题进行确认，这样的话就有时间来编造答案。仅仅通过犹豫来识别欺骗是不科学的，但它可以作为一个很好的信号源。有些人只是习惯于谨言慎行。我是纽约人，语速比较快。如果有人说话比我慢，并不一定都是在撒谎。你必须能够运用微表情去辨别他是真正说话慢，还是在试图编造答案。

如果他反馈的情绪和提出的问题不匹配，可能就值得推敲了。

3. 行为的变化

在交谈的过程中，每次谈到特定的话题，目标的行为都会发生变化。也许是表情的变化，或者是坐姿的改变，抑或是明显的犹豫。所有这些动作都具有欺骗的特征。虽然这些行为不一定等同于欺骗，但是你应该在不引起怀疑的情况下，继续深入这一话题。这些行为可能是一种信号，对方在利用时间的延迟来编造故事、回忆事实，或者决定是否要向你透露实情。

4. 手势

人们经常会用手势来描述场景。例如，用双手去比划某件物品的大小、某种物体运行的快慢，或者某件事被提及的次数等。许多专业人士认为，人在撒谎时会频繁地触摸或者摩擦自己的脸。从心理学的角度来看，这两者之间有一定的联系。网址www.examiner.com/mental-health-in-new-orleans/detecting-deception-using-body-language-and-verbal-cues-to-detect-lies中给出了一些心理学家和肢体语言专家关于检测欺骗的线索和暗示的讨论。

交谈过程中，留心观察手势的幅度、频率以及时长的变化很重要。不仅如此，做不同手势时的面部表情也要格外注意。

当你发现欺骗行为时，制定一个应对方案非常重要，也是个不错的做法。前面提到的场景中，当前台说CEO不在公司时，如果你当面指出她在撒谎，很可能会令场面陷入紧张状态，使她倍感尴尬，葬送一切可能成功的机会。如果你伪装的是权威人士，例如经理或者部门主管，抓住对方说谎可能会对你有利，因为你可以通过“原谅”对方让他欠你一个人情。但在同样的情形下，如果你的职位（比如是非管理岗位的秘书、接待员或者销售人员）低于目标人物，使用这种策略是很危险的。这种权威性的行为不适合非管理职位的伪装者。

综上所述，作为一名社会工程审计人员，必须学会观察他人的微表情，判断对方说的是实情还是谎言，并确定自己是否在按照想要的方式影响目标。在某些情况下，你甚至可以利用特定的表情操控目标的情绪状态。

记住，仅仅依靠微表情是不足以判断情绪产生的原因的。例如，即便能判断出目标是生气还是伤心，你也很难知悉个中缘由。在运用微表情的时候，需要细心谨慎地考虑各种因素，才能得出产生某种情绪的最可能的原因。

恶意社会工程人员会采用本节讨论的微表情技术，但是他们的目的和做审计的社会工程人员完全不同。他们往往不会顾及对目标的后续影响。如果破坏一个人的信仰体系、引发目标心理不稳定或者让目标失去工作会给他们带来利益，他们会毫不犹豫地去做。

前面章节提到过纽约“9·11恐怖袭击事件”之后发生的一些骗局。有些人不顾给他人造成的伤害，利用人们的同情心和灾难骗钱。许多人从阴影中走了出来，声称在这次袭击中失去了家人。这些充满恶意的人接受了捐助的金钱、礼物和同情，甚至引起了媒体的关注，最终却被人们发现他们的故事都是编造的。

恶意社会工程人员会花很多时间研究人，分析人们会因为什么上钩。这些知识会帮助他们找到易受攻击的目标。

本节谈及的微表情还较为浅显，该领域的专业著作称得上汗牛充栋。寻求培训，熟练解读和运用微表情，可以明显提升你与他人沟通的能力。此外，精通微表情会提高你的能力，从而在审计活动中获得成功。

5.3 神经语言程序学

神经语言程序学（NLP）研究的是人类思考和体验世界的结构。然而，由于NLP结构本身并不具有精确性或者符合某种统计公式，所以引起了很多的争议。很多科学家因此针对NLP的基本原则展开了讨论或辩论，但是NLP结构确实可以推导出运行框架模型。从这些模型中，又开发出

了可以迅速而有效地改变或限制人类思想、行为和信仰的技术。

根据维基百科（来源：《牛津英语词典》）的描述，神经语言程序学是“一种人际沟通模型，主要关注成功的行为模式和内在的主观经验（尤其是思想模式）之间的关系”，和“一种非传统的治疗系统，旨在教育人们要有自我意识和进行有效的沟通，并改变他们的心理和情绪行为的模式”。

因为这远非一本自助式图书，所以书中的内容虽然有助于你改变自己根深蒂固的思维模式和习惯，但是其重点还是如何运用NLP来理解和操纵周围的人。

如果不熟悉NLP，你的第一反应可能是找一台计算机，在谷歌中进行搜索。希望你暂时不要这样做。与社会工程学类似，你会首先发现很多看起来很不真实的视频和演示，例如视频中某人触摸另一个人的肩膀，就改变了这个人的大脑思维模式，以至于认为棕色是白色或其他颜色。这些视频使得NLP很神秘。对于那些持怀疑态度的人，这些类型的视频会让他们不相信NLP。

下面将NLP分解成几个部分。下一节是NLP历史的简短介绍，它有助于你理解NLP不是源于街头艺人，而是具有深刻的心理学渊源。

5.3.1　神经语言程序学的历史

神经语言程序学起源于20世纪70年代，由理查德·班德勒（Richard Bandler）和约翰·葛瑞德（John Grinder）在格雷戈里·贝特森（Gregory Bateson）的指导下提出。其根源是班德勒和葛瑞德对他们那个时代的一些最成功的治疗师的研究。

从这个初始研究起步，他们提出了NLP“准则”的概念。这一早期研究使元模型得到发展，元模型认为通过语言模式的使用能够对变化产生影响。

班德勒和葛瑞德当时都是美国加州大学的学生，他们使用研究中的原理，开发出了一种称为“元模型”的治疗模式。基于此模型的几本书出版后，他们开始细化其核心原理，最终形成了我们今天所说的NLP。这包括心锚（anchoring）、快速心态转变法（swish pattern）、换框法（reframing）、转变信念（belief change）、嵌套循环（nesting loop）、串联状态（chaining state）和次感元（submodality）的应用。

在拿到心理学学位之后，班德勒和葛瑞德开始举办研讨会和群体实践，这为他们提供了训练和测试新发现的模式的场所，同时允许他们向参与者传授技巧。在此期间，一群具有创新思维的学生和心理治疗师聚集在他们周围，为NLP学术作出了宝贵的贡献，使得NLP更加完善。

近年来，NLP成为了管理者的新流行语，使得这方面的培训人员、课程和专家群体快速增加。在没有管理机构的情况下，每个人都想学习控制他人、在撒谎时不会被拆穿，或者解决自己的心理问题，所以该领域不断发展。从业者没有执照，所以每个群组都教授他们自己的NLP形式和概念，并作为专家颁发自己的证书。所有这一切使得NLP给人们留下了糟糕的印象。