第二回 只是来看看

Wbth lal voe htat oy voe wxbirtn vfzbqt wagye C poh aeovsn vojgav?

有很多不那么虔诚的犹太家庭都很想为他们儿子举办一个成人礼（译注：这是犹太人的一种典礼，一般在男孩十三岁时举行，以象征他可以承担其成人的责任），我就是这么个例子。

这包括站在集会的前面阅读一段圣经旧约卷——用希伯来语。当然，希伯来语使用了完全不同的字母，比如  ，  ，  和类似的符号，所以学完旧约得花上好几个月的时间。

我在谢尔曼奥克斯（Sherman Oaks）的一所希伯来语学校注册登记了，但因为四处闲晃被踢了出来。

妈妈找到了一个诗班领唱来一对一的教我，这样我就不能躲起来在桌子底下读技术书籍了。我设法很努力的学习以应付礼拜，在集会时大声的读我的那一段旧约，不再像往常一样结巴，也不再让我自己丢脸。

后来我的父母都责怪我模仿拉比（犹太教祭司）的手势和口音，但这不是有意的。之后我了解到这是一个非常有用的技巧，因为人们很容易被和他们相似的人吸引。所以在很早的时候，我就已经在完全无意识的练习着“社会工程学”——有意或无意的影响人们去做那些通常不会做的事，说服他们而不会引起丝毫的怀疑。

家人和那些参与了成人礼之后在奥德赛餐厅的招待会的朋友给我带来了很多特别的礼物，包括一些美国长期债券（译注：美元），加起来相当可观。

我是一个狂热的读者，这种特殊的关注把我指向了一个叫做生存者书店的地方，那是在北好莱坞，一个很小很破旧的街区，老板是一个中年女士，有着一头金发并且很有友好，她对我说我可以直接叫她的名字。来到这个地方就像是发现了海盗藏宝的宝箱，那些日子我的偶像是李小龙，胡迪尼和吉姆• 罗克福德，由詹姆斯•加纳在《罗克福德档案》中扮演的冷酷的私家侦探，他会开锁，会操控别人，能在很短的时间内更换角色，扮演一个虚假身份的人，我也想像罗克福德那样做一些有趣的事情。

生存者书店有很多书描述了如何像罗克福德那样做巧妙的事，除此之外还有很多其它东西，从十三岁开始，我就花了很多个周末待在这里，一天到晚从一本书翻到另一本书——像是巴里•里德写的《文件之旅》，就讲述了如何用已过世的人的出生证明建立一个新的身份。

一本叫做《老大哥游戏》的书，作者是史考特•法兰西，就成了我的圣经，里面充斥着各种各样有用的东西，比如怎样获得驾驶记录、财产记录、信用报表、银行信息或者是未列出的数字，甚至是如何从执法门获得信息。（很久以后，当法兰西写续集时，他打电话给我问我是否可以写一篇文章，谈谈针对电话公司的社会工程学技术，那时候我的合著者和我正在写我们的第二本书，《入侵的艺术》，我实在是太忙了所以没能帮上法兰西的忙，虽然很巧合，但很荣幸。）

那家书店有很多“地下”书籍，教你一些你不应当知道的事情——对我而言

非常有吸引力，我一直有把禁忌之果咬上一口的冲动。我沉浸在这些后来成为无价之宝的知识中差不多二十年，直到我开始跑路。

书店里其它让我感兴趣的东西是他们出售的开锁工具，我买了好几种不同的类型。记得有一个老笑话，“你要怎么样上卡内基音乐厅？靠练习，还是练习，还是练习？”这就是我为掌握开锁技巧所做的事，有时候我会在我们那栋公寓楼的车库里打开一些储藏柜的锁，然后把它们交换，再把它们锁起来，当时我认为这是件很好玩的事，但回想起来，我想这很可能会把一些人惹恼，让他们陷入麻烦之中，他们在撬开旧锁之后还得买一把新的。我想，当你还是青少年的时候，这只是为了好玩。

当我差不多十四岁的时候，有一天，我和我叔叔米切尔一起出门，米切尔叔叔一直是我这些年来生活中闪亮的恒星。我们来到机动车管理部门，发现那里挤满了人。他让我等一等，然后径直走向柜台——越过每一个正在排队的人，DMV（美国车辆管理局）的员工，一个无聊的老太太吃惊地抬起头来。他没等她说完要到后面排队之类的话，就开始侃侃而谈，没用几句话，那个员工就开始频频点头，示意后面的人靠边一点，优先让米切尔叔叔办。我叔叔有一些与人打交道的特殊才能，

看上去我也有，这是我第一次认识到社会工程学的案例。 人们是怎么样看在门罗高中的我？我的老师们会说我总是会做让人意想不到的事，当其他小孩守在修理店的电视机前时，我跟随着史蒂夫•乔布斯和史蒂夫•沃兹尼亚克的脚步制造了一个蓝色盒子，用它我可以控制电话网络，甚至是打免费电话。我总是把我的业余无线电设备带到学校里，并在午餐和课间时间谈论这些东西。

但是有一位同学改变了我的人生道路，史蒂文•沙利塔，一个傲慢的家伙，总是幻想着自己成为一名卧底警察——他的车上到处都是无线电天线。他喜欢炫耀一些使用电话的小技巧，他可以做一些令人惊讶的事，比如他说他可以让别人不通过真实电话号码打电话给他，只要利用电话公司的测试线路：“环绕”（loop-around），他可以打电话给一个环绕线路的电话号码，其他人打给另一个环绕号码，这两个呼叫者会奇迹般的建立连接。他可以获得任何电话号码上绑定的名字和地址，不管是否在电话簿上，只要打个电话给客户姓名与地址管理局（CNA）。只用了一个电话，他就得到了我妈妈未公开的电话号码。

哇塞！他可以得到任何人的电话号码和地址，甚至是电影明星未公布的号码。看上去像是电话公司的人站在那儿随时准备为他服务一样。 我被吸引了，着迷了，然后我很快成了他的好朋友，我渴望了解所有这些难以置信的小技巧。但史蒂芬只热衷于给我展示他能做的事情，而不是告诉我怎样做才能像他一样用社会工程学技巧与人打交道。

没过多久，我就从他愿意分享的“电话截断”的一切开始进行自学，我几乎花了所有的课余时间去探索通信网络的奥秘，去发现那些甚至是史蒂芬都不知道的东西。飞客（phreakers）有一个社交网络，我开始接触其他有类似爱好的人，然后与他们打成一片，即便有些“飞客”有点，怎么说呢，比较怪——不善于交际并且一点也不酷。

我似乎应该剪掉关于电话盗打的社会工程学部分。我可以说服一家电话公司的技术人员在半夜开车到一个“控制室”（CO,central office——邻近的交换机中心，控制者附近所有的电话通路）连接一个“危险的”线路吗？就只是因为他认为我是另一个控制室的人，或者是片区的线路工人？太容易了。在这之前我已经有了这样做的能力，但是是我的高中搭档史蒂芬告诉了我这种能力有多强大。

基础战术很简单，在你开始针对特定目标的社会工程时，你得先侦查。搜集关于那家公司的信息，包括部门或业务单位是如何运作的，有什么样的职能，哪些是员工可以访问到的信息，进行申请的标准流程，他们通常从什么人那里接受申请，在什么样的情况下他们会发放被申请的信息，还有这家公司使用的行话和术语。社会工程学技术很容易生效，因为人们非常相信任何建立了可信度的人，比如得到了公司授权的员工。

这就是调查的用武之地，当我准备去弄未公开的电话号码时，我打电话给电话公司的商业办公室代表并说，“我是非公众部门（Non-Pub Bureau）的杰克•罗伯茨，我需要和主管谈话。”

然后线路被转接到主管，我再次进行自我介绍并说，“你有没有收到我们正在更改电话号码的备忘录？”

她查了一下，回到线上说，“不，我们没收到。”

我说，“你们应该打 213 687-9962。”

“不，”她说，“我这里写的是 213 320-0055。”搞定！

“好吧，”我告诉她，“我们会再发一份备忘录给二线”——这是电话公司的行话，意思是经理——“先慢点改，继续用 320-0055 直到你们收到备忘录吧。”

但是当我打到非公共部门的时候，我被告知我的名字需要在授权用户的列表上，还得用内部的回拨号码，这样他们才能把客户信息告诉我。一个新手或者不上档次的社会工程师可能就会挂了电话，这是个坏消息：引起了怀疑。

我即兴表演道，“我的经理告诉我他已经把我放在列表上了，我得告诉他你还没有收到他的备忘录。”

另一个障碍是：我得提供一个可以回拨的电话公司内部电话号码！

我不得不打给三个不同的商业部门，直到我联系上了一个经理，是个男的——我可以冒充。我告诉他，“这里是非公共部门的汤姆•汉森，我们正在更新我们的授权员工列表，你仍然需要在这个列表上吗？”

他当然说需要。

然后我要他拼出他的名字并给我他的电话号码，就像从婴儿那要糖果一样简单。

我的下一个电话是打给 RCMAC——最近内容更改授权中心（Recent Change Memory Authorization Center），这是电话公司用于处理添加或删除客户电话服务（比如自定义呼叫功能）的部门。我打电话冒充商业办公室的一名经理，说服一名员工给经理的线路添加一个呼叫转移是很容易的事，只要这个号码属于太平洋电话公司。

详细的说是这样的：我打电话给调度中心办公室的技术员，他相信我是一个片区的维修工人，他用线路工人手持机切入那个经理的线路，然后拨打了我告诉他的号码，为经理的电话设置了一个呼叫转移到电话公司的“环绕”线路上，环绕线路是一种特殊的回路可以让两个号码接通。当两边的电话都拨打相应的号码时，他们会奇迹般的连接在一起，就像是互相打电话一样。

我接入了环绕线路，第三方会听到听筒里的响声，当非公众部门回拨给那个已授权的经理时，电话被转接到环绕线路，打电话的人也会听到铃声。我让那人听了好几次响铃然后才接起电话，“太平洋电话公司，我是史蒂夫•卡普兰。”这下那个人就会愿意告诉我那些我正在寻找的非公共信息了，然后我回拨给调度技术员，让他把呼叫转移取消掉。

更大的挑战能带来更多的快感。上面的这一招多年来一直很有效，并且很可

能在今天仍然有效！

我花了时间分开打了几次电话——因为一次询问多个名人的电话号码会引起非公共部门的怀疑——我拿到了罗杰•摩尔、露西尔•鲍尔、詹姆斯•加纳、布鲁斯•斯普林斯廷和其他一些人的电话号码和地址。有时候我会打电话给一个明星，然后这样说，“嘿，布鲁斯，你还好吗？”没有任何恶意，只是能弄到任何人的号码让我很兴奋。

门罗高中有一门计算机课程，我没有修完前置的数学和科学课程，所以不能选这门课，推斯特老师（读“twist”）看到了我的渴望，认为我已经自学到了足够的知识，然后同意我上这门课。我想他后来可能后悔了：我是个难缠的家伙。

每一次他在学校的小型计算机上修改密码，我都会很快弄到。他破釜沉舟，极为圆滑的把他的密码打在了一张计算机纸带上，这种纸带是磁盘还未出现时的存储介质，他一直把这一小段打孔纸带放在他的上衣口袋里，透过薄薄的布料我都能看到里面的纸孔，我的一些同班同学帮我找出了纸带上这些孔的模式，每次他更改密码我们都能知道最终密码，他从未跟上过我们的脚步。

然后是计算机实验室的电话——很古老的，带旋转拨盘，这部电话被设置为只能拨打学校内部的号码，我开始用它拨入南加州大学（USC）的计算机玩游戏，我只要告诉接线员，“我是推斯特老师，我需要外部连接。”我打过很多次这种电话后接线员开始产生了怀疑，我就换用了电话盗打技术，接到电话公司切换并关闭相应的限制，然后我就可以在任何时候拨入 USC 了。最终他意识到我已经把这部电话的呼出限制给取消了。

不久他骄傲的在班上宣布他要怎样一劳永逸地阻止我拨入 USC，用一个专门为拨号电话设计的锁：当“1”号孔锁上时，它会截断电话的使用。

当他把锁设置好时，在全班的注视下，我拿起了听筒开始拨动转盘：快速地转九次“9”就接到了外部线路，再转七次“7”，四次“4”，不到一分钟，我就连接到 USC。

对我来说这只是一个斗智斗勇的游戏，但是可怜的推斯特老师觉得自己被羞辱了，他的脸刷的一下就红了，抓起桌上的电话扔到了教室的另一边。

与此同时我还在自学 RSTS/E（读作“RIS-tisEE”），这是数字设备公司（DEC）制造的一个操作系统，用在洛杉矶市中心学校的小型机上，临近的加州大学北岭分校（CSUN)也把 RSTS/E 用在他们的计算机上。我与计算机科学系的主席韦斯•汉普顿进行了会面，我对他说，“我对学习计算机非常感兴趣，我可以购买一个使用这些计算机的帐号吗？” “不，它们只对我们的已注册学生开放。”

放弃很简单，但这不是我的风格，“我那所学校的计算机实验室在每天下午三点的时候关闭，你能设置一个程序好让高中的计算机学生能在你们的计算机上学习吗？”

他拒绝了我，但是很快给我回了电话，“我们决定授权你使用我们的计算机，”他说，“我们不能给你一个帐号，因为你不是这里的学生，所以我决定让你使用我的个人帐号，用户名是‘5，4’，密码是‘Wes’。”

这个人是计算机科学系的主席，他给他的帐号设定了一个这样的密码？用他的名字？实在是太安全了！

我开始自学 Fortran 和 Basic 编程语言，在短短的几周计算机课程后，我编写了一个程序用于窃取别人的密码：他们看到的登录框实际上我伪装的操作系统界面，只要他们输入帐号和密码，就会被记录下来（类似于现在的钓鱼攻击）。事实上，在一台 CSUN 的实验室监视器上可以看到我在调试代码——可他们认为

一个高中生能知道如何窃取密码是个大笑话。一旦这个小程序开始运行在实验室的终端上，只要学生登录，他或她的用户名和密码就会被秘密的记录在一个文件里。

我为什么这么做？我的朋友和我认为能拿到任何人的密码是件很酷的事，没有什么邪恶的计划，就只是单纯的收集这些信息。只是如此。这是我从第一次看到魔术表演开始，整个早期生活中经常重复在做的另一件事。我能学会这样的技巧吗？我能学会糊弄别人吗？我能得到本不应该得到的权利吗？

一段时间以后系统管理员在一台实验室监视器上发现了我在做的事，接下来我知道的，就是三个校园警察以迅雷不及掩耳盗铃之势冲进了计算机实验室，他们把我关了起来，直到我妈妈来接我。

那个给我权限使用实验室并告诉我他自己帐号的系主席勃然大怒，但对此他没有什么可做的：在那时候，还没有相关的计算机法律条例，所以无法对我做任何惩罚。但是，我的权限被取消了，并且禁止我再到那里去。

我妈妈告诉我，“下个月会有一条新的加利福尼亚州法律，好让凯文知道他这么做是犯罪。”（在接下来的四年里，美国国会没有批准一些关于计算机犯罪的联邦法律，但我接下来一连串的动作被用来说服国会通过了新法案。）

在任何情况下，我都没有被威胁吓倒，在那之后不久，我就发现了一个可以转移打给查号台的电话的方法，在罗德岛打这个电话的人会被转接给我，你会怎么样从一个想得到某个电话号码的人那里获得乐趣？我日常的一个典型通话是像这样的：

我：城市？ 呼叫者：普罗维登斯。

我：姓名？ 呼叫者：约翰•诺顿。

我：商业用途还是普通用途？ 呼叫者：普通用途。

我：号码是 836，5，0.5，66。

这时候通常呼叫者会很困惑或者气愤。

呼叫者：我要怎么拨 0.5？！

我：买一台有 0.5 键的新电话。

我得到的回应非常滑稽。

那时候，两家不同的电话公司负责洛杉矶的不同区域，通用电话电子公司（GTE）负责圣•费尔南多谷的北部，那是我住的地方，任何距离超过 20 英里的电话会被收取长途费用。我当然不会像让我妈妈的电话账单跑飞，所以我都是用一个本地无线电补丁设备打的电话。

有一天我在电话里和广播电台的主持人神聊，他把我的电话标记为“奇怪的电话”，并注意到当我使用自动补丁时的一长串有规律的按键数字，我可以没有解释这些数字可以让我通过被称为 MCI 的长途服务商免费打长途电话。虽然他不知道我在做什么，但他不喜欢那一串数字，实际上是我用自动补丁造成的。一个收听了那次广播的家伙联系到了我，说他的名字是刘易斯•德•佩恩并给了我他的电话号码，我那天晚上打了电话给他，刘易斯说他对我在做的事情很感兴趣。

我们相识并成为了朋友，这种关系持续了至少二十年。因为阿根廷的血统，刘易斯很瘦很怪胎，留着很短很乱的黑头发，不漂亮也不强壮，还留着胡子，他可能是想让自己看起来年老一点。在黑客项目上，刘易斯是我在这个世界上可以信任的朋友，虽然他的个性充满矛盾，他很有礼貌，但总是想占上风。他是个书呆子，穿着一点也不时尚的毛衣和宽松的裤子，但还是风度翩翩，既低调又嚣张。

刘易斯有着和我相似的幽默感，我认为任何无趣且不能给人带来欢乐的业余

爱好都是不值得投入时间的，这一点刘易斯和我的步调一致。比如我们的“麦当劳大作战”就很有趣，我们找到了如何改造一个两米电台的方法，当顾客在快餐店的得来速（drive-through，免下车服务）点单时，我们的声音会在得来速的扬声器里响起来，我们前往靠近麦当劳但不会被注意的角落，开启手持式电台，把它调整到快餐店的频率。

一辆警车经过得来速车道，当他激活扬声器时，刘易斯和我说道，“对不起，我们这里不向警察提供服务，你得去 Jack in the Box（译注：一家美国速食连锁店）。”

有一次一个女人拿起听筒时听到扬声器里（我们）这样对她说，“把你的姐妹带来看看，你的巨无霸汉堡就是免费的！（titties 读音和 titty 很像，后者是乳房的意思）”她会错了意，下车来从尾箱抓出什么东西，冲进了快餐店……那是根棒球棍。

“免费苹果汁”是我最喜欢的恶作剧之一，在一个客户点完单之后，我们解释说制冰机坏了，所以我们免费赠送果汁。“我们有柚子味的、橘子味的和……喔，对不起，我们好像没有柚子和橘子了，你要苹果汁吗？”当客户回答可以的时候，我们就播放一段某个人往杯子里撒尿的声音，然后说，“好的，你的苹果汁准备好了，请开车到前面的窗口提取。

我们认为如果制造点难度让人无法下订单会是件很有趣的事，通过扬声器，每一次客户拿起话筒点单时，我们的一个朋友会重复他的订单，但是是用浓厚的印度口音，让人完全无法听明白，客人会说他没听明白，然后我们的朋友会说一些其它的同样让人听不懂的话，不断的重复——这会让客人一个接一个的抓狂。最妙的地方是我们说的所有话还会在外面的扬声器里传出，但是里面的员工却不会听到，有时候我们看到坐在外面桌子旁的顾客一边吃着汉堡一边笑，没有人能弄明白发生了什么事。

有一次，一名经理出来出来查看到底是谁弄乱了扬声器，他看了看停车场四周，挠了挠头，根本就没有人在那儿，也没有车，没有人躲在标志后面，他走到扬声器前，弯下腰，眯着眼仔细查看，就像是要在那儿找出个小人儿似的。

“你 XX 的在看什么？！”我用沙哑的嗓子吼道，他被吓得一蹦十英尺！

有什么我们在恶作剧时，住在附近公寓里的人会站在他们的阳台上跟着傻笑，甚至人行道上的人也乐得哈哈笑，刘易斯和我有时候会带上几个朋友，因为这实在是太热闹了。

好吧，是很幼稚，但那时候我才十六七岁。

有一些我的杰作就不那么纯洁了，我给自己设定了一条限制，就是进入到任何电话公司的地盘，都只是为了访问系统，或是阅读一些电话公司的技术手册。但是，就像他们说的，这更像是一种原则而不是限制。

1981 年的一个夜晚，那时我已经 17 岁了，我和另一个电话飞客（phone-phreaker）朋友史蒂•芬罗兹一起在外面玩，我们决定潜入太平洋电话公司的日落-高尔控制室，那是在好莱坞。从我们成为电话飞客开始，真身进入到电话公司内部一直就是从未被挑战过的禁区。访问那里得通过在门外的按键区输入正确的编号数字，我们用社会工程学很轻松的就获得这个编号，让我们光明正大的走进去。

我的上帝——这真刺激！对于我们而言，这就是个终极游乐场，但是我们应该找些什么呢？

一个穿着警卫制服的大块头正来回巡视这座建筑，和我们偶然相遇，他那样

子就像是夜店保镖或者 NFL 前锋（National Football League 美国国家足球联盟）。只是静静的站着什么也不做，他就能吓得你尿裤子，但不知何故，越是遇到这种状况，我就越是淡定。

我看起来还不大，远不像是一个可以进到这里的全职雇员，但我可不管这些。“你好，”我说，“今天晚上还好吗？”

他回答道，“还好，先生，我可以看看你的公司 ID 证件吗？”

我在口袋里翻了翻，“该死的，我肯定是忘在车里了，我这就去拿。”

他不吃这一套，“不，你们两个都跟我上楼，”他说，我们没有争辩。

他把我们带到九楼的交换机控制中心，在那儿其他员工正在工作。

心扑通扑通的跳，胸口起伏不定。

几个交换机技术员跑过来看发生了什么事，我想我唯一的选择是从这个警卫手里逃跑，但是我知道这样的机会越来越渺茫了。我绝望了，那感觉就像是已经和监狱一墙之隔了，但我还有社会工程学技巧。

我知道太平洋电话公司足够的名字和头衔，我打算小试身手，我解释说，“我在圣地亚哥的 COSMOS 工作（communications oriented multiuser operating system 通信专用多用户操作系统），我只是带我的朋友看看控制室是什么样子，你可以打电话给我的主管核实。”让后我给了他一个 COSMOS 主管的名字，感谢上帝给了我强悍的记忆力，但我知道我们看上去并不属于这儿，这个幌子其实很差劲。

那个警卫在公司内部目录上查找这个主管的名字，找到了她家的电话号码，然后打电话给她。叮铃铃，叮铃铃，叮铃铃，他先说很抱歉这么晚打扰您然后解释了现在的状况。

我说，“让我来跟她说。”

他把电话递给我，我把听筒凑得很近，祈祷他不要听到她的声音。我即兴捏造了一些东西，“朱迪，打扰你实在是很抱歉——我带着我的朋友参观交换机中心，但把我的公司 ID 证件给忘在车里了，警卫只是来核对我是从圣地亚哥的 COSMOS 中心来的，我希望你不要因此怨恨我。”

我停下来一会儿，就好像在听她说一样，她在咆哮，“你是谁？我认识你吗？“你在那儿干什么？！”

然后我说，“只是我必须在早上赶到新培训手册的讨论会，我和吉姆在星期一的上午十一点有一个审查会议，如果你愿意顺便来参加的话，我们还是在星期二一起吃午餐，对吧？”

再次停顿，她还在咆哮中。

“当然，很抱歉打扰您，”我说。然后我把电话给挂了。

警卫和交换机技术员看上去很困惑，他们还指望我把电话还过去，好让那个主管亲自告诉警卫一切正常。你真应该看看那个警卫的表情：他还有胆子再打过去打扰她吗？

我告诉他，“她不是很高兴，我们在凌晨两点三十分叫醒她了。”

然后我说，“我只有几样其它东西想向我朋友展示了，我只要十分钟。”

我走了出去，罗兹紧紧地跟着我，当然我也想用跑的，但是我知道这不行。

我们到了电梯，我重重地按下到一楼的按钮，离开大楼后我们俩都松了口气，刚才实在是太危险，差点被吓得尿裤子，真高兴顺利离开了。

但是我知道会发生什么事，那位女士会不顾一切的四处打电话，深更半夜询问有谁知道怎样获取日落-高尔控制室警卫办公室的电话。

我们回到了车里，我开着车到了街对面，大灯也没开停了下来然后我们坐在那儿，盯着大楼的前门。

大概十分钟以后，大块头警卫出来了，他装着到处找我们的样子，心里以为我们早跑了，可惜，他错了。

我等他回到大楼里便开车闪人，在过了一个路口后才打开大灯。

这实在是太险了，如果他打电话给警察，罪名将是非法入侵，甚至更糟，入室盗窃。史蒂夫和我将被关进青少年管教所。 近段时间我是不会再回到电话公司的地盘了，但是我真心希望能有一些别的什么——更难的东西——来挑战我的智慧。