**十度分隔法**

黑客社会工程学攻击的八种常用伎俩著名黑客KevinMitnick在上世纪90年代让“黑客社会工程学”这个术语流行了起来，不过这个简单的概念本身（引诱某人去做某事，或者泄露敏感信息）却早有年头了。专家们认为，如今的黑客仍在继续采用黑客社会工程学的新老伎俩盗窃密码、安装恶意软件或者攫取利益。

**此处所列的是一些最流行的利用电话、email和网络的社会工程学攻击伎俩。**

**1.十度分隔法**

利用电话进行欺诈的一位社会工程学黑客的首要任务，就是要让他的攻击对象相信，他要么是1）一位同事，要么是2）一位可信赖的专家（比如执法人员或者审核人员）。但如果他的目标是要从员工X处获取信息的话，那么他的第一个电话或者第一封邮件并不会直接打给或发给X。

在社会心理学中，六度分隔的古老游戏是由很多分隔层的。纽约市警察局的一位老资格探员SalLifrieri，如今正定期举办一个叫做“防范性运营”的企业培训课程，教授如何识别黑客穿透某个组织的社会工程学攻击手段。他说，黑客在一个组织中开始接触的人可能会与他所瞄准的目标或人隔着十层之远。

“我讲课时不断地在告诫人们，多少得具备一些放人之心，因为你不知道某人到底想从你这儿获得什么，”Lifrieri说。渗透进入组织的起点“可能是前台或门卫。所以企业必须培训员工彼此相识。而作为犯罪起点的秘书或者前台距离犯罪分子真正想接近的目标有可能隔着十层之远。”

Lifrieri说，犯罪分子所用的方法很简单，就是奉承某个组织里更多可以接近的人，以便从职务更高的人那里获得他们所需的信息。“他们常用的技巧就是伪装友好，”Lifrieri说。“其言辞有曰：‘我很想跟您认识一下。我很想知道在您的生活中哪些东西是最有用的。’然后他们很快就会从你那里获得很多你原本根本不会透露的信息。”

**2.学会说行话**

每个行业都有自己的缩写术语。而社会工程学黑客就会研究你所在行业的术语，以便能够在与你接触时卖弄这些术语，以博得好感。“这其实就是一种环境提示，”Lifrieri说，“假如我跟你讲话，用你熟悉的话语来讲，你当然就会信任我。要是我还能用你经常在使用的缩写词汇和术语的话，那你就会更愿意向我透露更多的我想要的信息。”

**3.借用目标企业的“等待音乐”**

Lifrieri说，成功的骗子需要的是时间、坚持不懈和耐心。攻击常常是缓慢而讲究方法地进行的。这不仅需要收集目标对象的各种轶事，还要收集其他的“社交线索”以建立信任感，他甚至可能会哄骗得你以为他是你还未到这家企业之前的一位同事。另外一种成功的技巧是记录某家公司所播放的“等待音乐”，也就是接电话的人尚未接通时播放的等待乐曲。“犯罪分子会有意拨通电话，录下你的等待音乐，然后加以利用。比如当他打给某个目标对象时，他会跟你谈上一分钟然后说：‘抱歉，我的另一部电话响了，请别挂断，’这时，受害人就会听到很熟悉的公司定制的等待音乐，然后会想：‘哦。此人肯定就在本公司工作。这是我们的音乐。’这不过是又一种心理暗示而已。”

**4.电话号码欺诈**

但最分子常常会利用电话号码欺诈术，也就是在目标被叫者的来电显示屏上显示一个和主叫号码不一样的号码。“犯罪分子可能是从某个公寓给你打的电话，但是显示在你的电话上的来电号码却可能会让你觉得好像是来自同一家公司的号码，”Lifrieri说。于是，你就有可能轻而易举地上当，把一些私人信息，比如口令等告诉对方。而且，犯罪分子还不容易被发现，因为如果你回拨过去，可能拨的是企业自己的一个号码。

**5.利用坏消息作案**

“只要报纸上已刊登什么坏消息，坏分子们就会利用其来发送社会工程学式的垃圾邮件、网络钓鱼或其它类型的邮件，”McAfeeAvert实验室的安全研究主任DaveMarcus说。Marcus说，他们的实验室在这次的美国总统大选和经济危机中看到了此类活动的增多趋势。

“有大量的网络钓鱼攻击是和银行间的并购有关的，”Marcus说。“钓鱼邮件会告诉你说，‘你的存款银行已被他们的银行并购了。请你点击此处以确保能够在该银行关张之前修改你的信息。’这是诱骗你泄露自己的信息，他们便能够进入你的账户窃取钱财，或者倒卖储户的信息。”

**6.滥用网民对社交网站的信任**

Facebook、MySpace和LinkedIn都是非常受欢迎的社交网站。很多人对这些网站十分信任。而最近的一次钓鱼欺诈事件就瞄上了LinkedIn的用户，这次攻击让很多人感到震惊。Marcus说，已经有越来越多的社交网站迷们收到了自称是Facebook网站的假冒邮件，结果上了当。“用户们会收到一封邮件称：‘本站正在进行维护，请在此输入信息以便升级之用。’只要你点进去，就会被链接到钓鱼网站上去。”Marcus因此建议人恩最好手工输入网址以避免被恶意链接。并应该记住，很少有某个网站会寄发要求输入更改口令或进行账户升级的邮件。

**7.输入错误捕获法**

犯罪分子还常常会利用人们在输入网址时的错误来作案，Marcus说。比如当你输入一个网址时，常常会敲错一两个字母，结果转眼间你就会被链接到其他网站上去，产生了意想不到的结果。“坏分子们早就研究透了各种常见的拼写错误，而他们的网站地址就常常使用这些可能拼错的字母来做域名。”

**8.利用FUD操纵股市**

一些产品的安全漏洞，甚至整个企业的一些漏洞都会被利用来影响股市。根据Avert的最新研究报告，例如微软产品的一些关键性漏洞就会对其股价产生影响，每一次有重要的漏洞信息被公布，微软的股价就会出现反复的波动。“公开披露信息肯定会对股价产生影响，”Marcus说。“另有一个例子表明，还有人故意传播斯蒂夫·乔布斯的死讯，结果导致苹果的股价大跌。这是一个利用了FUD（恐慌、不确定、怀疑），从而对股价产生作用的明显事例。”

当然，反向操纵的手法也会发生，这很像以前的所谓“哄抬股价”的伎俩。垃圾邮件的发送者会购买大量的垃圾股，然后伪装成投资顾问疯狂发送邮件，兜售所谓的“潜力股”。如果有足够多的邮件接收者相信了这一骗局并购买了这种垃圾股，其股价就会被哄抬起来。而始作俑者便会迅速卖空获利。