信息库建立：

本科生的大创系统设计参与大创的人信息泄露，在<input>里面，设计网页的人真是懒。除了好看点，这网页真是又渣又卡。

微信公众号上可以获取一些信息，比如宝岛眼镜的账号主体是“上海苏博眼镜有限公司”

思考直接向目标索取信息的可能性，骗局不一定非要弄的复杂以防止被人识破

间接索取可以了解到更多的消息比如专业术语

行为：

通过“环回”电话（打xxxx电话到我的办公室）获取目标号码。

让对方高兴是拉近距离的一种手段，比如打电话表示对服务满意。

利用同情、内疚与胁迫，whoami电影的例子里面男主通过因丢失老爸钱包被其狠揍的样子，进入了政府内部餐厅，在桌子下方安装了可远程连接设备（远程连接靠运营商）（可扫描、攻击范围内的wifi）。

冒充遇到了不小麻烦的同事，如果能够知道某一个人的名字或者相关的专业术语那就更好了，人们容易亲进与自己相关的人，相比较陌生人。常见的是数据丢失叫同事帮忙查询信息。

公司曾经的员工是很危险的，可能现在的程序留有后门比如URP系统改成绩事件，还可能引发社工问题。

公司、学校、实验室的新人一般容易受到帮助。

无关信息总是容易被获取的，比如只有对公司内部人员有用的信息，认为外面的人拿到也没有用，但是这个可是冒充身份的一部分。比如公司内部没有公开的电话。

专业术语在SCU里面可以是本科系统的500 Server Error，讲出这个就基本可以认为你是一个本科学生了，不过老师一般不知道系统这个问题。网上面可以找到文档描述公司内部数据库系统的使用信息，或者哪些信息可以被提供给xxx部门（这时候就可以冒充部门来索取信息，进行进一步冒充）。二基楼的鬼故事，公司的丑闻。

长相、声音、衣着也是关键，就像好看的女生容易获得好感，一个小孩就容易套话。

假装是猎头，对公司状况进行询问（业内用语）

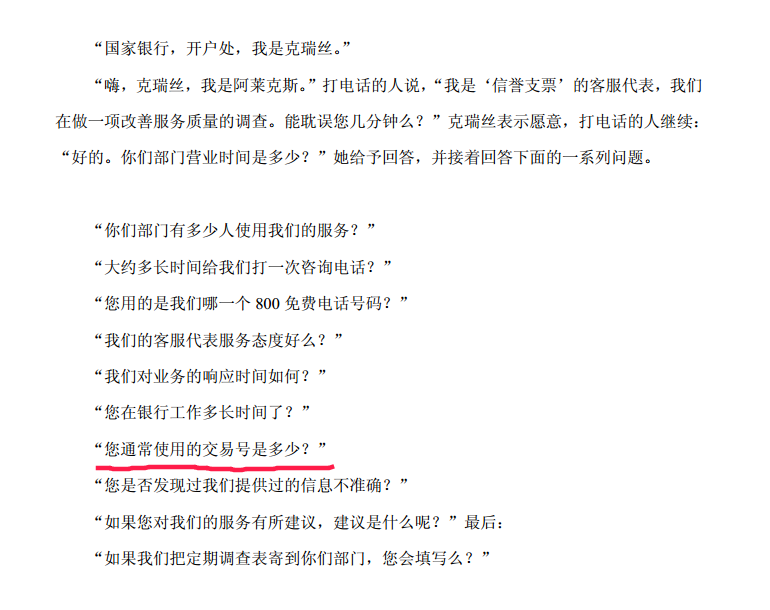
用户往往受过培训，不信任HTTP前缀的网站。

公司以及内部人员（高层）丑闻

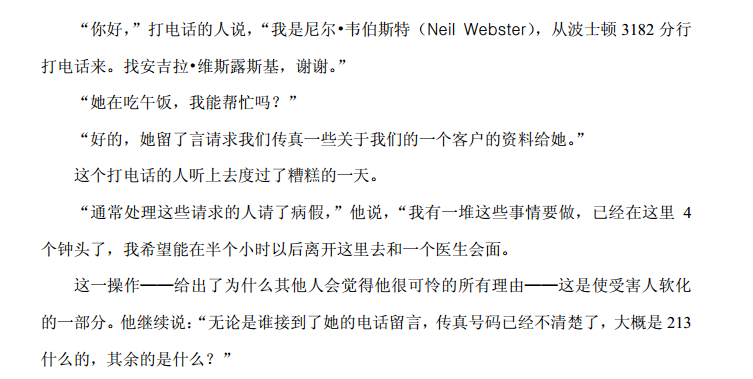
email的自动回复邮件会暴露什么“正在海外旅游”，然后就可以被冒充了。

员工满意度调查，前50名可以获得xxxx

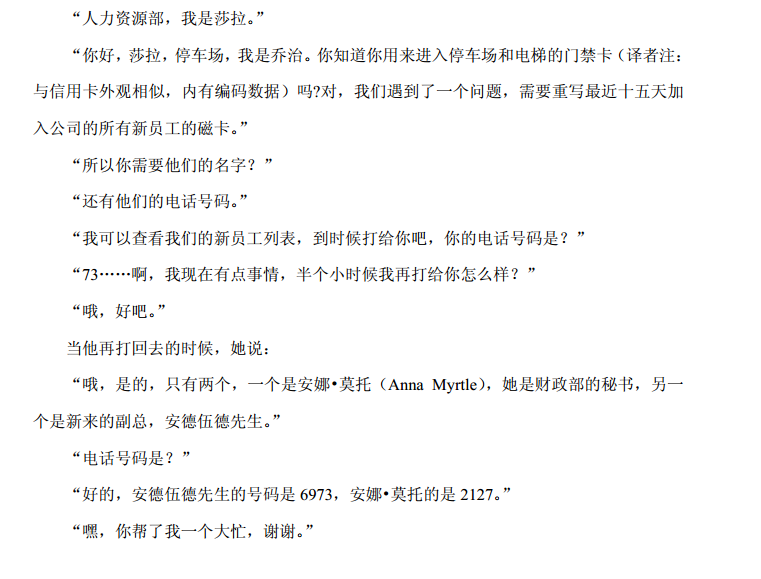
遗落的U盘、CD，甚至是被贴上“员工年度考核”“第几季度员工精简提案”标签的媒介。



不仅仅是交易号、生日信息等全都是可以询问的，然后就可以使用这些足够的信息来冒充这一个人。《欺骗的艺术》中的例子，其中“交易号”这个专业术语是以出书为借口套出来的。在询问交易号之前，先问了一个关于工作多长时间的私人问题，没有引起警觉才继续询问了交易号。



没想到是软化，从一般人的角度来讲就是拒绝。



直接将公司的一条电话线路呼叫转移到自己的电话上，比如这是条查询数据库信息的服务员线路（警方向后台索要罪犯信息），然后就能愉快地询问了。

生气的样子，别人一般不会去接近你。

密码安全检查：

https://haveibeenpwned.com/ 需要输入账号或者邮箱

https://shuju666.com/

mimayun.club

社工攻击工具：

setoolkit（social engineering toolkit）简称SET：产生社工攻击向量的频繁跟新工具

可以通过修改/usr/share/setoolkit/config/set\_config来扩展功能

Select from the menu:

1) Social-Engineering Attacks

2) Penetration Testing (Fast-Track) 类似于Metasploit操作

3) Third Party Modules #包含远程管理工具Remote Administration Tool RAT，可以嵌入游戏等

4) Update the Social-Engineer Toolkit

5) Update SET configuration

6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

攻击载荷里面的PyInjector与MultiPyInjectior直接向内存注入Shell代码，而不接触磁盘。Materpreter还需要安装。

网站、邮件、SMS（short message service）、传染性媒体、Ardiuino、无线热点

Spear-Phishing Attack Vectors鱼叉式网络钓鱼攻击，最终会渗透目标系统

Java Applet一旦被运行，网页就会重定向到原始网站。如果单击取消，脚本将重新出现而不能关闭浏览器，除非杀死进程。

Credential Harvester就是采集用户的输入凭据，可以通过site clone的方式。

Mass Mailer Attack 指定邮件列表来发送大量邮件，做到钓鱼攻击，不同于鱼叉式，多数是为了获取用户信息，比如盗号。

Arduino xxxx 将Arduino编程为鼠标、键盘，一旦插入就会自动运行并打开后门。

Create a payload and listener 就同msf了，SET会调用msf。

Tabnabbing Attack Method ：web模板、站点克隆、定制化导入

web jacking attack method web劫持（配合DNS欺骗使用，会说原本的站点已经改变了然后诱导你点击一个连接进入一个自己制作的钓鱼或者攻击页面）

有文件生成的话就会在当前目录下的.set/

Fast Track：

python开发，与SET同作者

1) Microsoft SQL Bruter

2) Custom Exploits

3) SCCM Attack Vector

4) Dell DRAC/Chassis Default Checker

5) RID\_ENUM - User Enumeration Attack

6) PSEXEC Powershell Injection

99) Return to Main Menu

不管那种测试（白盒、黑盒），与多个用户交流可以得到不错的信息。

我们来到客户的工作场所进行进一步的内部测试，与最终用户展开交流，询问他们是否再使用新安装的系统时遇到什么问题。出人意料的是，他们谁（注意这里这一个问题问了很多个人）都不允许我们碰触他们的系统，很快解释说因为这里存在登陆问题，一段时间内不允许连接超过10次。后来一个成员发现一位老员工使用互联网遇到了问题，我们询问他是否需要帮助，告诉他可以用我们带来的笔记本连接到局域网，然后身后的一个同事用摄像笔记录了老员工的所有操作，包括登录系统的账号。

还有个女士告诉我们经常在登录的时候遇到问题，然后我们告诉他我们将尽快解决，但是需要她的账户信息与登录ip。

---------------------------------------------------------------------------------------------------------------

解雇以后会安排人员护送着出去，防止摧毁设备或者数据