从手机号出发：

第一步：百度得到手机的归属地和运营商，百度和Google得到手机周边的各类信息[[1]](#footnote-1)。

第二步：社交账号搜索。微信→支付宝→QQ→新浪微博

利用手机号弄到微信号（因为大部分微信号都是通过手机来注册的），并基于第一步的信息（当然也可以结合后面的步骤）尝试虚构验证信息，如果对方警惕性弱甚至可能进入其朋友圈。

这一步在利用支付宝的转账功能方面有一个小技巧：在选择转账时会显示对方名字（如果对方支付宝已验证并实名制的话），并且支付宝会提供姓的窗口供转账者验证，如果基于其他信息可以判定出姓（或者直接暴力猜解）则我们就确定了机主姓名。

最后人肉验证一下查到的网站以及其他大网站（如网易的163, 126, 微信, 新浪微博等）。

第三步：破解第二步查询到的用户密码，特别是邮箱密码，优先考虑纯社工路线，如果是英文邮箱可以尝试在panda pants里搜索，（不过如果是基于手机注册的话一般都是数字邮箱，没有办法检索panda pants），或者利用第一步得到的信息或者简单猜测法搞定密保问题。

1. 这一步很重要，是后面过程中社工的基础，可以多尝试几个搜索引擎。 [↑](#footnote-ref-1)