一部手机失窃而揭露的窃取个人信息实现资金盗取的黑色产业链

速读摘要

家人一部手机被盗，自己经历一场与一伙专业老练的利用窃取个人信息盗取他人银行账户资金的犯罪团伙的持续斗争，把这个比作一场战争，显然自己败了，败得没那么惨而已。除了短信验证码，支付宝的快捷绑卡还验证了下支付密码，但好像意义也不大，比如我这种情况，支付账号都是别人用我的信息新建的，支付密码也是他设置的。这样手机丢了也不用担心别人拔下卡插其他手机里继续使用。也不一定哈，9月5日我们补办完手机卡时我就和我老婆说了，后面这段时间内要小心陌生的电话和短信、微信。

原文约 8061 字 | 图片 17 张 | 建议阅读 17 分钟 | 评价反馈

一部手机失窃而揭露的窃取个人信息实现资金盗取的黑色产业链

原创 信息安全老骆驼 信息安全老骆驼

作者简介：

信息安全老骆驼，10多年网络攻防工作经验，多年金融信息安全服务从业经历。理工直男，不擅文字，一直在信息安全行业默默无闻。

近日，由于家人一部手机被盗，自己经历一场与一伙专业老练的利用窃取个人信息盗取他人银行账户资金的犯罪团伙的持续斗争，把这个比作一场战争，显然自己败了,败得没那么惨而已。但以一己之力对抗一个分工明确、手法专业的团伙，且能在败后分析揭露对手的攻击方法、路径，虽败，犹荣。第一次码这种文章，没有华丽的文字，只有流水账本的叙述，但其中情节跌宕起伏，一波三折，愿意的朋友可以当成故事看完，嫌啰嗦的也可以直接拉到最后看总结。

这篇文章的发布，可能会让一些人不高兴，但相较广大民众的财产安全，这又算什么呢。如果我不把真相告诉大家，相信会有更多的人中招，稀里糊涂钱就没了。

事件回顾：

9月4日

7:30 正带着大娃在理发店理发，老婆过来告诉我，她在小区门口推着二娃蹲下买水果时婴儿车袋子里的手机被偷了。这是看到P40 pro上市，一年一度的换机季又到来了。说是丢失后就用其他手机拨打，但对方接通后关机。当时不知道我怎么想的，觉得可能还有机会能找回，没有未立即挂失手机卡，设置了华为找回手机的上线通知（这个不果断的决定，导致了后续悲剧的发生）。

8:51 对方把卡取出来插在其他手机开机，后面通过查询通话和短信详单才知道，才一个小时多点的时间，对方从高新区直奔成华区，以周五成都高峰期的交通状况，算是比较极限了。

9:24家人发现被偷手机可以拨通，但我这边“查找我的手机”显示还未上线，但没两分钟我的手机收到提示手机在成华区上线了，瞬间再看找回手机界面，设备被解绑了，突然有种不好的感觉，一般的小偷不会这么快这么熟练的干这些。立刻致电10000号挂失手机卡，但此时电信服务密码已经不正

确了，通过验证身份证号码加提供上个月联系过的三个电话号码进行了挂失。开始采取紧急措施，登录手机银行把可立即赎回的理财全部赎回，活期余额全部转我账上，联系多家银行冻结信用卡，把支付宝、微信上的资金转走，绑定的信用卡全删掉，考虑到部分储蓄卡余额为0，且对方不知道我的卡号，就没去挂失。

9:48 家人说电话还可以打通，立马致电10000号，询问为什么还可以拨通，回复说卡是正常状态，继续挂失。

9:55 越想越不对劲，又致电10000号，问之前挂失失败的原因是什么。得到答复，第一次挂失是成功了的，但后面又被**解挂**了。还有这种操作，打电话解除挂失，我是第一次知道，常识性认为我挂失了就应该是带上身份证去营业厅解除挂失，包括后面去报案，民警听说挂失后还可以电话解挂，也是很惊讶。但明显对方是有备而来，后期分析时我认为连偷手机的时间都是事先定好的，对方把电信的业务流程已经掌握得很清楚了，这也导致我后期的补救措施变得很被动。

根据云闪付上的绑卡信息，继续给银行电话，挨个冻结储蓄卡，建行etc信用卡因为已经解绑了，且第二天要出行上高速，就没去管了。这期间还漏掉一个老婆10多年前办的一张建行卡，一张工商银行卡，又埋雷了。

00:23时，发现支付宝、微信接连被挤下线，重要的是登录的设备和丢失的手机设备型号一致！完了，遇上高手了，华为的锁屏密码被解开了。立马申请冻结（后面发现，已经晚了，对方的操作很迅速，此时支付宝已经被更换了手机号码，怀疑是多人在并发操作的。）、同时申请冻结微信，马上登陆京东，苏宁、国美等常用的APP，更换关联手机号码。没过一会，我的手机就收到一条京东的短信验证码，感觉后面几个APP应该是保住了（蜜汁自信，最后还是被打脸），喘一口气休息下。

分析对方意图，觉得所有银行卡和支付余额里偷不到钱的话可能会用老婆的信息申请贷款，但同时想到放款只能是放到本人银行卡，要想转出去得有银行卡密码（长期以来自己支付密码和银行卡密码一致，连自己都忘了这两个密码不是一个东西，后面追查时才发现，对方用了一个神招，什么银行卡密码、支付密码根本影响不到对方），应该问题不大，加上期间紧张于电信手机卡“挂失”、“解挂”阵地抢占，又有张成都银行社保金融卡漏下了。

后面一晚上就是循环的的我挂失、对方解挂，在10000号上来来回回几

十次。至于为什么要坚持，因为觉得虽然自己已经把重要的APP和银行账户都保住了但还是看不透对方想干什么，不过既然对方这么执着的解挂我的手机卡，肯定是有其迫切的原因。抱着凡是敌人想要的，就坚决不能给的信念，一晚上通宵坚持下来了。这期间我们是很被动的，因为捕知道他什么时候解挂，只能躺床上不停打被偷的电话，一拨通立马再打10000号挂失。

中间多次请求10000号客服，告知手机被偷，犯罪分子正在解挂手机卡用于实施犯罪，请求他们通知领导获得审批后冻结手机卡等明早去营业厅补卡，都被拒绝。由于一晚上几十次的业务办理，甚至还被客服说“**你们自己的私事，不要占用公共资源**”，我都不知道对方是怎么忽悠客服的。询问还有没有其他途径自助办理挂失，回答无。只能继续坚持，最后不知道是不是客服自己都受不了我们了，10000发短信告诉我可以在网厅自助办理，登录电信网厅，尝试用软件自动挂失，无奈网厅的一些安全限制导致无法用软件实训自动化的挂失办理，继续手动操作。

5:00发现才注意到网厅有关闭短信的业务，想着如果对方是高手，我关闭后也可能对方会立马发现，但也可能对方只是流水线的犯罪脚本操作工人，可以赌一赌，反正对我没损失，对他们还增加开通短信的步骤。（后面查短信详单时发现，正是关闭短信功能这个操作，中断了他们后续的犯罪行为，不然损失肯定更严重）

熬到9月5日9点，开车送老婆蹲守营业厅开门，9点8分完成补卡，丈母娘来电话说老婆电话打通了，但接电话的是个男的,我回答说可能是营业厅的营业员接的。几分钟后老婆办卡归来，问到刚才丈母娘电话什么情况，她说没接到电话啊，手机一直在自己手上。看了下确实没有通话记录，手机外拨也是正常的，短信发送接收也正常。继续打10000号，询问手机是否被开通了呼叫转移，得到确认的答复，验证身份证后关闭业务。关闭之前从话务员那边问到被转移的电话号码（准备后续万一要报警就提交过去）。

开始收复阵地，检查损失。找回支付宝、微信、云闪付，发现除了支付宝手机号被改了，但由于账户本身冻结状态，就没管了，。从云闪付上管理的银行卡里交易记录基本没什么异常，只有一张工商银行卡多了280元（诡异吧），一看是从一个钱袋宝 转过来的， 觉得蹊跷下了个APP想用手机号码登录钱袋宝看下，APP异常，登录不上。暂时就没管了。

约了朋友一起峨眉山泡温泉，喝下一瓶乐虎、一瓶红牛、一瓶咖啡，出发去峨眉山，途中继续检查了了下各个支付账户，好像没什么异常。下午到了峨眉山，在温泉池子里休息，恢复体力。准备晚上从电信营业厅查下详单，看对方都干了什么。

晚上查详单前老婆登录支付宝结果习惯性输入手机号码，发现密码错误， 赶紧用手机找回，突然想起自己支付宝账号不是手机号，一看才发现是对方新建的支付宝账号，还绑定了那张被我们遗忘的建行卡，以及一张建行ETC信用卡（办好etc后就一直在抽屉里吃灰），而且账单里有充值消费记录，以及被支付宝风控阻断后的充值退回记录，这时候才发现这张原本绑在云闪付上的信用卡被对方从云闪付解绑了，所以我们才没发现异常。登陆建行网银，发现9月5日4点多时美团转进 5000元的记录，跪了，再看etc信用卡有各种买卡、充值 的记录 几大千，银联转账记录几大千，最坏的情况还是发生了。

下载了短信和通话详单，开始分析通话和短信记录，挨个查询，基本上

通话的都是各家银行、银联，短信记录能查的到源号码的也就是 社保局、华为、腾讯、银联、翼支付、微信、支付宝，其他106开头的服务号不知道是哪个机构的，分析没什么结果。

两人开始回忆从头到尾的细节，开始逐个分析，一个资深渗透测试工程师的优势这时候展示体现出来了。对方第一次上线时已经把卡拔出来插到其他手机，从短信发送记录上看是给一个手机发了条短信，获取到本机手机号码。然后联系电信改了服务密码，用手机号码配合短信验证码改了华为密码，把原设备上的账号注销了。然后解锁了华为锁屏密码，进入了手机。这中间有几个说不通的地方：

1.修改电信服务密码需要身份证号码

2.有华为密码从网站上也没有解锁锁屏密码的功能。

第一个我想的是可能从社工库查到了身份证号码，第二个根据百度结果说是华为老版本的emui 账号登录后可以远程锁机，设置一个新密码，然后用新密码解锁屏幕进入手机（这个操作未实际验证）。

然后对方还修改了支付宝登录和支付密码、微信密码，中间还修改了支付宝手机号码（为什么这么操作到9月7日晚上的分析才知道），并且绑定了被我们遗漏的银行卡至支付平台账号上进行消费。这里又有说不通的地方：

1. 支付绑卡需要银行完整的卡号，如何得到的？一开始以为打银行客服就可以问到，后面试了下是不行的；

但当我查看支付宝的银行卡管理功能时，发现有支付密码的话，可以用支付宝自带的查看卡号功能获取银行卡完整卡号，太长时间没用这个功能了。

但这样的话就还有个说不通的：

支付密码的重置需要的条件（1.人脸 2、短信+安全问题 3、短信+银行卡信息 4 银行卡+安全问题），没照片的情况下，人脸应该不行，我们设置的安全问题基本上不会被猜到，那只有短信加银行卡了（实际上最后发现，对方既可以人脸验证，也可以短信加银行卡验证，甚至连支付宝都是自己新建了一个，支付密码也是自己设置的）。

然后剩下的步骤就比较清晰了，通过绑了卡的美团，申请贷款，放款到建行储蓄卡再通过支付APP之前的绑卡结果，通过购买虚拟卡和网络充值消费掉。

剩下就是苏宁金融的信用卡消费了，还是抱着怀疑的态度，他们如何搞到我的信用卡cvv的，这一点我们是比较肯定的，etc信用卡从申请下来就没离开过抽屉。从银行客服那边能获取到的最多也就是信用卡有效期。（后面才发现支付公司现在绑信用卡根本不验证有效日期和CVV，都是简单粗暴的身份信息+卡号+预留手机号码，甚至有些连预留手机号都不用）。

整理完所有的情况后，就准备联系各个支付公司，准备讨要说法了。一圈下来后，得出的结果是：

1. 银联云闪付态度极好，说第二天会有专人联系
2. 财付通 联系不上
3. 美团借贷 态度模糊 ，问他为何只是简单验证了身份证就放款了，只说这种贷款产品很多其他公司也有的，嗯好像很有道理，大家都做的就是正确的。

4. 苏宁金融未回应

准备好一些材料，包括通话、短信记录、银行账单，以及其他零散资料，准备赶回去报警。毕竟事情发生在小区门口，而且团伙作案，极有可能还会再犯，把事情整理下发到业主群，让大家小心防范，提醒大家设置好sim卡密码。大家也都被震惊了，但一致对于怎么获取身份证号码、银行卡号表示疑惑。中间手机陆续还收到几条财付通的支付验证码，但登陆自己账号，没发现有绑卡，留着疑惑后面再处理，反正不给验证码也付不出去。

思路理清楚了，已经凌晨4点多了。一早赶紧往成都赶。路上云闪付主动联系我们，让我们报警后提供报案回执单等一些材料提交过去，看样子有可能要赔付。美团也打电话过来了，想推卸责任，但还是让我们提供证据资料提交给他们。派出所民警听说了我们的遭遇都表示惊奇，说之前从没遇到过这种偷手机的。我应该是第一个来报这种案件的 。老婆进去做笔录，耗时几个小时， 出来后说了里面的情况，警察大叔们都表示“这不可能”、“肯定是你手机里放银行卡信息泄露了”、“你是不是放身份证照片在手机里了”，做完笔录竟然又要我们去打印银行流水，跑了几家建行 都是关门的，只能等第二天再来取报案回执单了。

晚上回去两口子在电脑前继续回想所有细节，把整个过程串一遍，必要时用我的各种APP和账号进行实验，验证自己的分析判断。虽然补了手机卡， 银行卡都冻结了，带支付功能的软件都找回来各种修改密码了，但总觉得哪里就是不对劲。突然又收到了财付通的支付验证码请求，再关联起前面的几个可疑点，一下子想通了。 **他用其他支付账号绑了我们的银行卡，**包括之前用手机号登陆苏宁时发现登陆的是别人新创建的苏宁账号、包括支付宝也是新建的，至于他们新建的的账号怎么通过的人脸实名认证，这个留在后面讨论。说明除了这些APP，肯定还在其他一大堆APP上用我的信息新建了账号，绑了银行卡、通过了实名认证，并自己设置了支付密码。挨个APP检查， 发现用我们的手机号码新建了支付宝、苏宁、京东且包含有消费记录，这个操作隐蔽性强，如果我们没发现的话，解冻了银行卡，他们还可以用自己创建的支付账号进行消费。

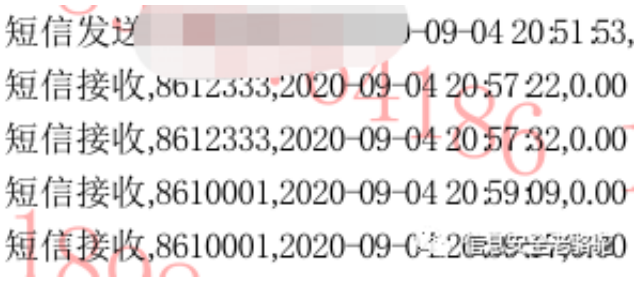
问题又来了，他们用我的手机号新建的账号 我们可以挨个试出来， 但用其他手机号新建的账号我们猜不到，比如云闪付、财付通、苏宁金融 ，这几个从银行流水里查到有转账消费记录，但我们没找到对应的账号。

再回到上面有疑惑的几个问题上：

1. 要在支付宝上查看我绑定的银行卡信息或者绑新的卡，需要支付密码而支付密码的重置，需要短信+一张银行卡信息的验证
2. 一开始整个环节的起点，都需要我的身份证号码，期初我判断是通过社工库，但这一番操作分析下来，整个黑产团队的手法，基本都是利用的各个银行、支付公司的正常业务流程来处理的，那么身份证的获取大概率也不会采用社工库去查询；
3. 部分支付APP新建账号后的实名认证，需要活体人脸验证，这个如果可以从手机自拍照或者华为云里之前存过的照片，用技术处理手段处理照片绕过人脸识别（参考2020年的新闻《利用照片伪造动画头像“骗过”支付宝人脸识别，一犯罪团伙薅支付宝“羊毛”超4万元》）

总结下来就是，需要有一个地方，通过手机号码和接收到的短信验证码， 能获取到姓名、身份证号码、以及一张银行卡的卡号

感觉这几天自己都有点病态了，遇到这种盗刷的倒霉事，不愤怒、不沮丧、不慌乱，而是出奇的亢奋，几天下来没睡几个小时，不停的研究和分析，快把对方的运作模式研究出来了，把IT男追根刨底的特质发挥的淋漓尽致。



来，继续冷静分析，手头能跟犯罪分子行为步骤关联最紧密的就是电信营业厅获取的短信和电话记录了，翻出短信记录，除了第一条犯罪分子发给自己手机号的记录，紧接着就是收到两条12333社保局的短信。最开始两天都没注意到，以为是老婆公司给缴纳的社保的通知短信，但再仔细分析就发现不对劲了。一是短信发送时间可疑，非工作时间内发送社保缴纳通知是不正常的，连发两条也是不正常的，那突破点就是它了，社保系统里肯定是有身份证信息。

打开四川省人社厅的网站，看到一个四川人社的APP下载二维码，下载打开APP的瞬间就明白了，“快捷登录”、“短信验证码”、“电子社保卡”这几个关键字明晃晃的扎我眼。

发送短信验证码，登录进去。点开“电子社保卡”，发现需要社保密码，继续忘记社保密码，短信验证码重置社保密码，这一切刚好是两条12333的短信验证码，随后展示在眼前的内容，直接解释了上面三条疑惑。身份证信息、证件照片、社保金融卡的银行卡信息，有了这些东西，干啥都一路畅通了。

再返回去之前的支付宝绑卡流程，“无需手动输入卡号，快速绑卡”，几年没用绑卡功能，现在都这么高端了。选一家银行点进去后，该银行下我的所有银行卡列表直接出来了，选上信用卡，绑卡。CVV 、有效期 这些都是浮云，人家就一个简单的短信验证码验证，这样的话通过支付宝查看你所有银行卡的卡号就简单了。

最后我们再来总结分析一波：

这条黑产链的全貌如下：

1. 一线扒手特定时间选定目标：年轻人、移动支付频率高，在对方注意力分散的情况下出手，运营商营业厅下班后，失主没法当晚立即补卡，给团队预留了一晚上的作案时间；
2. 拿到手机后迅速送到团队窝点，迅速完成身份证信息获取、电信服务密码、手机厂商服务登录密码修改，一下子让受害者陷入被动；
3. 获取所有银行卡信息，使用技术手段绕过活体人脸识别验证，在各个平台上创建新账号，绑定受害者银行卡
4. 选好几家风控不严的支付公司，开始申请在线贷款，贷款到账后通过虚拟卡充值、购买虚拟卡以及银联转账，将钱转走
5. 保留新建的支付账号权限， 如果未被发现，后期还可以继续窃取资金

在这一系列过程中，对方有几点还是让我比较服的：

1. 全程用的都是正常的业务操作，只是把各个机构的“弱验证”的相关业务链接起来，形成巨大的破坏；
2. 应该是使用了技术手段通过的人脸验证，用图片处理技术来绕过活体人脸识别验证；
3. 团队分工协作能力太强，在处理过程中我感觉自己已经用了最快的速度，但总还是晚一步。
4. 注重隐蔽，留好后路，包括删掉我云闪付上的一些卡来防止我查明细，通过新建账号的方式，如果我没发现，贸然去解冻银行卡，后续还有第二波的攻击；包括赶在我补卡后改服务密码前，设置了呼叫转移

分析完犯罪分子，再来看下整个过程中参与的机构都有什么“罪”，实际上这个环节里的每一个点，放在对应的业务节点里都不是什么大问题，但手机丢失后，把所有这些点串起来，问题就大了：

1. 四川电信： 我认为整个过程责任最大的就是它了，这挂失、解挂的风骚业务规则简直让我无语，既然都挂失了，不应该考虑到手机已经不在失主身上了，解挂不应该有个时间限制或者要求营业厅办理么？就算前面的过错无视了，同一个手机号码在深夜来来回回挂失解挂几十次，包括机主几次在电话中告知话务员自己正在遭受银行卡盗刷犯罪，要求停止解挂行为，话务员还是拿着业务话术来敷衍客户“对不起，我们的挂失解挂有固定的业务流程，只要对方能提供服务密码，正常就是可以解挂的”。我们全家人就这样抱着电话陪犯罪分子熬了一夜，到最后还是造成了经济损失。对于四川电信，后续该投诉投诉。
2. 四川人社： 它所起到的作用，大家也都看得懂。两条短信验证码，关键的资料全泄露出去了，但我不好说他有什么罪，毕竟他们本身也不是金融机构， 对个人信息的保护要做成什么样也没个标准。但这个事情没那么简单，把四川人社换成XX人社或者四川XX，也可能是一样的结果，这个黑产链设计的时候身份证号码的获取途径可以是多处的，至少我随便在网上下载几个地方社保APP，都能找到和四川人社一样登录和密码找回使用手机短信验证的。

3. 华为 ： 其实把华为换成小米，结果也是一样。我只能说密码找回这个业务的验证太简单了，还有就是网上说的用emui 5.0的手机，可以远程解锁屏幕锁屏密码，这个我没验证过， 但从我支付宝被挤下线时提示对方使用的手机型号来判断，大概率是可以的。

4. 支付宝：先不说为啥同一个身份信息，可以注册两个账号，你的快捷

绑卡，是加快了绑卡的便捷性， 但考虑过安全性么？当然，支付宝的风控是强，确实识别到了异常交易，也追回了资金。但实名认证的人脸识别被绕过，也是事实。

5. 美团：你要发展业务，放宽贷款限制，这我不关心，但你能否做好该有的贷款审批风险控制，凌晨4点的贷款行为，这正常么？

6. 苏宁金融：所有参与这个过程的支付机构中态度最恶劣的一家，出现案件，接到用户报案后第一时间想到的是推卸责任。“报案了么？如果警方有需要，我们会做好配合工作！哦你的经济损失啊，那只能你自己承担了”，中间来过两次电话，基本腔调就是这样。同样是支付公司， 支付宝的风控能识别异常盗刷，苏宁金融就一点察觉都没有，一个新注册的账号，凌晨三四点绑卡，然后购买各种虚拟卡、充值话费这些不容易被追查的商品，这不算高风险异常行为么？

7. 银联云闪付: 和其他支付公司一样， 都存在绑卡验证不严的问题。但是，人家态度是好的啊，凌晨3、4点，客服人员都能用极好的态度和我们沟通，让我们放宽心。第二天有专员联系我们，告诉我们昨晚报的损失少报了，他们查出来我们还有其他损失，并给了详细的指引告诉我们怎么去申请理赔，第二天他们内部调查有新的进展也都第一时间联系并告知我们。

8. 财付通：人工客服太难找了，不过风控也还是有效的，这两天在没有通知我们的情况下，陆陆续续追回了几笔交易金额。

9. 京东：不想说了，反正就是“交易已经发生了，损失你自己承担”，但还好就一笔100元的游戏充值卡。

10. 百度 对方刚好操作到它的时候短信功能已经被我关了，对方也只是绑定了银行卡，还没来得及消费，就不用找它理论了。

多数支付机构基本都有一个现象：允许用不同的手机号码注册相同实名认证的支付账号，允许两个账号绑定相同的银行卡，实名认证有人脸活体识别技术的都被绕过了。支付机构都在推“快捷绑卡”，是快捷了，点几下鼠标就绑卡了。除了短信验证码，支付宝的快捷绑卡还验证了下支付密码，但好像意义也不大，比如我这种情况，支付账号都是别人用我的信息新建的，支付密码也是他设置的。

说完他们，最后再来说说咱们吧。通过这几天的经历，不管中间情节有多少起伏，我作为一个有10多年信息安全从业经验的老骆驼，都要被折腾成这样，我实在是不想让大家有跟我相同的经历。提个我认为我们个人能做的

最简单最有效的防护措施：

给自己的**手机卡上个密码**，给手机设置个屏幕锁。这样手机丢了也不用担心别人拔下卡插其他手机里继续使用。以华为手机为例：设置-安全-更多安全设置-加密和凭据-设置卡锁， 选定手机卡，启用密码（此时使用的为默认密码1234或者0000），再选择修改密码，输入原密码1234，再输入两次新密码，完成sim卡的密码设置。

同时，如果有遇到和我一样情况的，除了冻结所有银行卡后，还需要把银行卡的预留手机号码全换掉，同时可以通过登陆网银或者手机银行，用快捷支付管理功能，查看都绑了那些支付公司，然后可以尝试用自己的手机号码去登陆那些APP，，有可能还会有意外收获，万一支付公司不给理赔，还能自己追回一点。比如我就在对方注册的苏宁账号上找到还没来得及消费的购物卡。

然后这个事情是不是就这样结束了？也不一定哈，9月5日我们补办完手机卡时我就和我老婆说了，后面这段时间内要小心陌生的电话和短信、微信。对方快吃进嘴的肉被硬扯下去一大块，手里又有你的一些信息，肯定不会甘心的，要小心后续的网络钓鱼、和电话诈骗。这两天她手机就开始收到有可疑的短信了，什么套路也懒得去猜了，反正不理会就是了。

我所经历的这个案件，其实和前两年新闻上报道过的钱包丢失，对方用偷到的身份证去营业厅补了卡，然后导致银行账户损失其实是差不多的，目标都是手机卡。移动互联网的发展给我们的生活带来了巨大的改变，手机的地位也越来越高，希望大家吸取我的这次经验教训，提前做好防范，出事别学我，第一时间挂失手机卡、所有银行卡。

文章已于修改