2020年6月24日 星期三
责任编辑:张海 编辑:马俊杰 十堰晚报

“什么都没做，一觉醒来就发现自己的银行卡被洗劫一空。日前，海南三亚警方破获了一起新型银行卡盗刷案件。不法分子是如何无声无息地把钱转走的？又该如何防范？

■据《成都商报》




# 什么都没做，银行卡被隔空盗刷？

## 当心！你的验证码被“嗅探”了

### 没进行任何操作 银行卡被转走5万元

2019年7月4日凌晨3点多，海南省三亚市宋女士的手机上突然收到了几条短信验证码。不一会儿，手机又接到短信，显示她的银行卡被刷走了5万元。钱被转走前，宋女士根本没有进行任何操作。于是，她赶紧到附近的三亚市公安局三亚湾派出所报案。接到报案后，民警展开调查，发现宋女士的钱从广东惠州一家银行的自动取款机上被取走。于是，警方很快锁定了犯罪嫌疑人并将其抓获，宋女士的5万元被全部追回。

虽然钱被追回来了，但警方有个疑问一直无法破解，宋女士没有进行任何操作，那么不法分子是如何盗刷宋女士的银行卡呢？警方成立专案组对此案进行深挖，经过连日奋战，这个作案人员涉及海南、四川、山东、广东等地，成员有着严密分工、单线联系的特大网络盗刷团伙终于现形。2019年7月，专案组民警在湖南娄底抓获了这个团伙的上家陈某华。

据犯罪嫌疑人供述，他们在三亚有一个同伙，在宋女士居住地附近，嗅取了宋女士的动态支付验证码。然后他将动态验证码发给洗钱通道，于是便将宋女士的钱给取出来了。

### 15元的旧手机 被改造成“嗅探”设备

犯罪嫌疑人顾某某交待，通过改造摩托罗拉118的手机，把它变成一个接收天线，再配合特定的U盘系统，打开电脑就可以模仿基站信号，拦截、嗅取探测周围手机短信。一部手机15元，相当于一个简单的拼接过程。

为什么如此简单的设备，却能截获大量的手机短信呢？据中国政法大学网络法学研究院副院长王立梅介绍，这与受害人手机的网络信号有关。虽然现在早已进入4G时代，但信号不好时，手机还是会切换到2G网络。另外，一些犯罪嫌疑人会利用信号干扰设备，将一定范围的手机信号降为2G。王立梅表示，在2G的状态下，加密技术相对来讲比较简单，比较容易破获。

要想将受害人银行卡上的钱转走，犯罪嫌疑人必须同时获得该用户的姓名、身份证号、银行卡号、手机号和动态验证码。那么犯罪嫌疑人又是怎么获得用户完整的银行卡号呢？顾某某说：“可以随便点一个充值方式，看付款方式，可以看见你所有的卡。”确定作案对象后，犯罪嫌疑人会利用受害人的手机号码加动态验证码，使用免密支付的方式将受害人的钱转移出去。

### 银行卡被盗刷莫惊慌 及时冻结可避免损失

顾某某还表示，用户在一些App上实名注册信息，很多时候是图方便，忘记密码的时候可以通过短信验证码登录，这同时也方便了犯罪分子盗取用户的个人信息。

当用户忘记密码的时候，可以通过手机号发送验证码的方式找回密码。这一切对用户来说似乎很方便，也很安全。可是不法分子恰恰利用这种登录方式，选择在夜深人静、人们防范意识比较低的时候，在自己的手机或电脑上输入用户的手机号，再用截获的动态验证码登录用户的App，达到盗窃用户资金的目的。

王立梅表示，手机号加验证码的方式本身是有一定的安全隐患，验证码是有可能被截获的。第二个就是预留的手机号码，这个号码泄露的可能性非常大，所以两个加在一起，作为唯一的验证方式是有一定漏洞的，尽可能应该是再有其他的验证方法予以补充。

公安机关提醒，普通用户应加强个人防范。当突然收到不明验证码，发现银行卡被盗刷不要惊慌，及时报警，冻结银行卡可以避免损失。

