

央视网消息（焦点访谈）：银行卡被盗刷，这事挺可怕。海南三亚警方就破获了这样一起新型银行卡盗刷案件，一位女士在家什么都没做，一觉醒来，却发现自己的银行卡已经被洗劫一空。像这样一类盗刷案件已经多次发生，引起了人们的关注。那么，不法分子是怎么无声无息就把钱转走了？这类案件为什么会多次发生，我们又该如何防范呢？

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。

在银行卡上的钱被转走之前，宋女士有没有进行什么操作呢？有没有什么可疑的事情发生呢？

受害人宋女士说：“没有任何操作，问你的身份证，你的银行卡密码，根本就没有，根本不用我操作。”

什么都没有操作钱就被转走了，宋女士赶紧到附近的三亚市公安局三亚湾派出所进行报案。接到报案后，接案的民警也感到蹊跷。

因为整个过程受害人没有和盗刷银行卡的人有过任何的沟通、接触，无法提供盗刷银行卡的人的任何信息，于是三亚警方决定从资金流向入手展开调查。

三亚市公安局天涯分局三亚湾派出所副所长赵成良说：“宋女士的钱从银行卡出来以后，我们查询到这笔钱进入到了通联支付公司，就是第三方支付公司。这笔钱从通联支付底下一个第四方公司，叫广州冠胜，有一个代付业务，发起了一个收款请求。”

最后，这笔钱从广东惠州一家银行的自动取款机上被取走，三亚警方很快锁定了犯罪嫌疑人，在广东惠州将其抓获，宋女士的5万元钱被全部追回。钱被追回来了，这个案子或许到此已经可以结案了，但警方在侦破过程中有一个疑问却一直无法破解。以前的一些案例，不法分子掌握了受害人的个人信息后，会设法获取受害人的银行卡密码进行转款。而本案受害人宋女士的钱被转走是因为与动态验证码被截获有关，这个似乎更安全的动态验证码不法分子是怎么获取的呢？

三亚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，专案组民警开始收网，在湖南娄底抓获了这个团伙的上家陈某华，抓获现场几台电脑还正在运行。

赵成良说：“当时我们就问他，这个动态验证码是怎么获得的？他说是在三亚有一

个同伙，在被害人居住的范围之内，嗅取了被害人宋女士的动态支付验证码，嗅取到以后他将动态验证码发给洗钱通道，就将这个钱给支付出来了。”

什么是嗅探？犯罪嫌疑人又是怎么嗅取了受害人的动态验证码的呢？

犯罪嫌疑人顾某某说：“用摩托罗拉118的手机，通过一番改造，把它变成一个接收的天线，再配合上特定的优盘系统，在电脑打开之后，就可以模仿基站信号，拦截相当于嗅取探测到周围手机短信。一个手机15块钱，相当于一个简单的拼接过程。”

为什么如此廉价简单的嗅探设备就能截获大量的手机短信呢？

中国政法大学网络法学研究院副院长王立梅说：“在2G的状态下，因为加密技术相对来讲比较简单，比较容易破获，或者容易破解，那么当到2G这种网络的时候，嗅探技术在中间截获这个数据包，然后解开就可以了。”

虽然现在我们早已进入4G时代，有的地方甚至已经用上了5G，但在一些4G信号不好的地方，手机会切换到2G网络。另外，一些犯罪嫌疑人利用信号干扰设备，专门对一定范围的手机信号进行干扰，这时这些用户的手机信号也会突然变成2G信号。这些犯罪嫌疑人就会利用2G网络存在的漏洞，用嗅探设备吸附到周围一定范围内的手机信号。吸附成功后，受害人的手机号码和短信会自动显示在犯罪嫌疑人的电脑上，受害人不会有任何察觉，悄无声息中就变成了犯罪嫌疑人的猎物。

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、动态验证码。这5个条件就像5把钥匙，一般情况下犯罪分子很难获得，但因为有了受害人的手机号码并能够实时截取动态验证码，犯罪嫌疑人就如同拿到了一把“万能钥匙”，他们会通过网络来获得其他几把钥匙。

对于一些没有买过保险，或者在淘宝没有登记信息的用户，犯罪嫌疑人会同时登录这个用户其他的多个APP。

最关键的是支付环节，不少APP往往都会对用户的银行卡号刻意隐去几位，那么犯罪嫌疑人又是怎么获得完整的银行卡号呢？

顾某某说：“可以通过充值，我随便点一个充值的方式，立即充值和付款方式，可以看见你所有的卡。我知道你有建设银行的，我就可以去跑你的卡，就脚本跑你的卡，像招商银行的和工商银行，我直接通过别的APP就直接获取了。你也不用惊讶，这也不是我发明、创造的，就是这么一种操作的方式。”

犯罪嫌疑人获得了受害人的姓名、身份证号、手机号、动态验证码、银行卡号这些信息之后，还会挑选作案对象，查验用户是否有作案价值。

确定了有价值的用户之后，犯罪嫌疑人会再次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。

此时，受害人什么都没有操作，手机上会收到一堆验证码，之后银行卡上的钱就被转走了。这个案件当中，犯罪嫌疑人使用的嗅探设备十分廉价，嗅探技术也不是什么高深的技术，为什么却能屡屡得手呢？

顾某某说：“你在一些APP上面去实名注册信息，很多时候是图方便，当你忘记密码的时候，就可以通过短信验证码去登录，这个时候你会感觉到很方便，同时也方便了我们这些犯罪分子去盗取你的个人信息，通过验证码登录，方便了你，也方便了我。”

记者随后在手机上，选择了多个常用的APP进行测试，这些APP一般都可以通过用户名加密码和手机号加动态验证码两种方式进行登录。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手机号加动态验证码也可以登录的便利，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。

王立梅说：“手机加验证码的方式可能是现在大多数的，尤其是在网络空间这种很多APP所通行采用的方法，不是说一两个通行验证方式，但是这种验证方式本身它是有一定的安全隐患的，也就是说首先验证码是有可能被截获的，这是其中一个。第二个就是预留的手机号码，这个号码实际上它泄露的可能性也是非常大的，所以它们两个加在一起，做一个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。”

不仅如此，很多互联网公司对用户的个人信息保护也不到位。

王立梅说：“在我们登录很多很多APP，使用很多移动服务的时候，每一个移动服务都要求我们提供一遍我们个人的一些数据，那么当我们进入这么多的使用了这么多的用途以后，几乎我们所有的信息，就在互联网各个节点有非常多的备份，那么任何一个备份丢失、泄露等等，都会造成全部数据的遗失。”

因为犯罪嫌疑人能够故意干扰手机信号，这样就会使4G和5G手机自动转到2G网络。而2G网络的先天不足一时难以弥补，这就要求众多互联网公司和银行不能以手机加动态验证码作为唯一的身份验证方式，应该尽可能再增加其他验证方法予以补充

。同时，普通用户也要加强个人防范。

犯罪嫌疑人陈某某说：“最好的办法，打个比方，你如果说要绑定第三方平台银行卡，尽量不要放太多资金。”

当用户突然收到不明的验证码，然后发现银行卡被盗刷了也不要惊慌。

赵成良说：“第一时间到公安机关报警，及时止付，把你的银行卡挂失冻结，我们公安机关去追这笔钱。”

这个案件虽然不大，但反映出来的问题值得大家关注。我们的个人信息就像水池里的水，每使用一项互联网服务就像给这个水池安装了一个管道，增加了泄露的风险，更令人担忧的是，很多管道用的都是同一种水龙头，手机号码加验证码。现在信息网络技术犯罪越来越多，这些不法分子之所以能够得逞，就是利用了网络技术上的各种漏洞。人们希望电信运营商、互联网企业、银行以及监管部门能多想办法，保障人民群众的财产安全。毕竟，没有安全的方便是没有意义的。