在没开通相关网络支付等功能的情况下，犍为杨先生的银行卡竟在一夜之间被盗刷124笔，损失了6万多元。这是怎么回事？5月18日，银行方面表示，事发后已及时协助客户追回了2671.14元。目前，警方已介入调查。

50多岁的杨先生是乐山犍为人，工资卡是单位在某银行集中办的。他称，3月18日中午他到附近银行查询发现，工资卡里的6万多元只剩下几十元了。他赶紧让银行工作人员挂失该卡并打印流水账单，随后报警。银行提供的交易记录显示，从3月17日20时44分至3月18日4时33分，杨先生的银行卡被盗刷了124笔，总金额60671.15元。除了几笔是通过pos机交易外，剩下的上百笔全部是在某电商平台通过“中间业务后台”渠道，从其活期账户上以490元每笔的方式转走。另外，杨先生的银行卡没开通网银，预留电话开通了余额变动提醒，但杨先生表示，3月17日、18日并未接收到任何余额变动提醒。

疑似木马病毒拦截消息

3月18日，银行员工向杨先生的手机尝试发送短信，其手机确实无法正常接收短信。对此，银行工作人员猜测，他的手机可能中了木马病毒。根据杨先生打印的事发当天短信往来记录显示，事发时银行确实向其预留的手机号码发送了短信，但几乎每次发送短信后，杨先生的手机又向一个“150”开头的手机号码发送了短信。

对此，有专业人士分析称，一般情况下开通余额变动提醒功能后，如果银行卡内的资金变动银行会通过短信的方式告知客户，如果开通快捷支付，也会向预留手机发送验证码进行验证，如果杨先生手机中了病毒，这些短信都被拦截了，会自动转发给犯罪分子。

对此，杨先生称，自己对智能手机功能并不完全了解，所以确实有可能误点了什么链接，中了木马病毒，但他认为，自己没开通网上银行、网络支付等功能，银行卡被盗刷，银行也负有一定责任。5月18日，当事银行相关部门负责人表示，初步来看可能是客户手机中病毒导致的，银行不负有责任。事发后银行已帮助杨先生追回2671.14元。银行工作人员也会同杨先生将其手机封存后移交给了当地警方，请求对该手机是否中病毒进行技术鉴定。目前，警方正在做进一步调查。

近些年，银行卡被盗的事情频繁发生，融小妹提醒广大卡友，一点要注意以下几点：

方法一：伪基站发送钓鱼短信

很多人都有过相同的遭遇，就是收到了类似10086、95533等所谓的电信运营商或银行发来的短信，登录后被要求输入密码。

其实都是犯罪分子利用伪基站“包装”后发送给用户的含有钓鱼网站的短信。仅360平台上监控到的钓鱼网站，半天时间就有超过1亿次的点击量。在这些钓鱼网站的虚假网页上，用户登录后就会被要求输入账号、密码、姓名、身份证号、银行预留手机号等信息，而一旦填写了这些信息，骗子就可以把用户的钱骗走了。钓鱼网站的更新速度非常快，每天都有5000到8000个新的钓鱼网站被监测到。

方法二：免费wifi窃取个人信息

除了使用钓鱼网站获取个人信息，犯罪分子还会利用免费wifi窃取个人信息。

一个wifi的安全性主要取决于它的架设者是谁，如果是骗子或者是黑客架设了一个免费wifi，用户一旦接入，所有互联网的数据都可以被黑客监听或窃取。

方法三：改装pos机提取银行卡信息

除了以上两种获取信息的方式，黑市中的犯罪分子还有第三种方法——那就是利用改装的pos机提取用户银行卡信息。在黑市中，pos机提取的信息被称为“轨道料”，数量上要远远少于钓鱼网站上提取的信息。但是卖价却很高，余额较大的信息甚至可以卖到几千块钱一条。

而对于这些信息，犯罪分子通常会等半年以上才把信息出售，目的是让消费者积累大量pos机消费记录，这样警方就无法追查是哪台pos机提取了银行卡信息。

完成了“下料”的工作，在这个黑色产业链上，下一步就是将受害者银行卡里的钱转出来，犯罪分子把这个步骤称为“洗料”。这也是很多受害者最疑惑的地方——我的钱究竟是怎么没的?下面就跟随记者的调查，一起揭开这个谜底。

起底拦截短信验证码两种方法

在qq群中，每天都会有很多人发“洗拦截料”的广告。这些人被称为“洗料人”，他们可以把受害者银行卡里的钱转出到“料主”指定的卡号里，从而获得30%到50%的提成。而他们主要关注的就是用户短信验证码。

方法一：让手机中毒拦截验证码盗取钱财

验证码是金融机构在用户进行诸如修改密码、转账等操作时，向用户预留手机号码中发送的一次性的密码，没有验证码则无法进行转账等操作。而要想获取验证码，犯罪分子最常用的手段就是向目标手机里发送木马。文章开头的吴先生就是手机只要受害者点击木马程序，手机短信内容就会被犯罪分子拦截。犯罪分子通过事先掌

握的银行卡主的个人信息将银行卡绑定在第三方支付平台，然后把钱转走。而此时受害者的手机既收不到消费提醒也收不到验证码，卡里的钱就这样被转走了。

方法二：近距离干扰手机信号拦截验证码

让手机中病毒是最为常见的拦截验证码方式，然而却不是唯一的方式。记者发现在黑市中，已经有人不需要木马病毒就可以拦截验证码。他们的方法就是通过特殊的改装设备对手机信号进行干扰，但这种方法有一个限制条件，那就是这个设备就必须处在目标手机一公里范围之内。因此，使用这种拦截方式必须要靠近受害者。那么，犯罪分子要怎么确定目标的位置呢?其实这个很简单，一般的手法就是给那个目标打电话，说你自己是送快递的，你这个地址写得不是很清楚，让他把地址再说一遍，只要他把地址说出来，我们就能在一公里范围之内拦截他银行卡的验证码。

发现银行卡被盗刷你该这么做

发生银行卡被盗刷，这样做才对：冻结卡片，防止损失继续扩大——拨打客服挂失或者通过手机银行自行操作。多数银行有“失卡保障”服务，在挂失前48或72小时发生的盗刷可赔付。

立即报案

立案回执要保存——这样在向银行主张权利时才有据可查。

留取证据

正确的做法是：立刻到附近银行取现，并打印凭证。这样做是为了证明银行卡在你手中，而其他地方没有卡。

嘘！融资攻略问答频道与大家正式见面了，专业的信贷经理随时解答你的疑问，欢迎大家随时提问，提问请戳>>>>我要提问！