近日，一名北京网友发布的“为什么一条短信就能骗走我所有的财产?”的文章在网络广为传播。据该网友爆料，她收到一条“订阅增值业务”的短信，根据提示回复了“取消+验证码”后，半天之内支付宝、银行卡上的资金被席卷一空。到底是什么样的电信诈骗手段完成了这一卑劣的盗窃行为呢?

收到垃圾短信她回复“退订” 半天内财产被席卷一空

“噩梦” 回复短信TD退订而引发

“4月8日，周五，下班回家地铁上。我的手机忽然收到一条短信：显示来源为‘1065800’的号码发来了一条短信杂志，这种垃圾杂志看多了，我第一反应是回复‘TD’。该短信回复我‘发的指令不正确’。”

文中信息显示，随后该用户相继收到显示为“10086”，以及“10658139013816280086”发来的信息，提示已开通“中广财经半年包业务”，“如需退订请编辑短信‘取消+校验码’至本条短信退订”。而在另一条显示来源为“10086”的信息中，该用户收到“尊敬的客户，您的USIM卡6位验证码为******”。此时，该用户压根儿不知道USIM卡验证码是什么，于是回复了“取消+******”。

此后，该网友的支付宝、支付宝所绑定的银行账户陆续发生转账。

“时间太短。”该网友写道，“所有卡挂失完成，已耗去大半小时。我知道支付宝和银行卡里所有的钱都没了。”

该网友第二天到各个营业厅打印交易流水确认“两张卡都已空空如也。”更确认“对方”“不但攻破了支付宝的账号，连各个银行的网银也逐个攻破”，包括163邮箱密码也被篡改。其间还包括，“对方”在该用户完全不知情的情况下，将“三张银行卡都绑定关联了百度钱包”，用于转账。

调查 移动确认办理“业务”IP在海口

昨日下午，北京移动在核查之后就上述事件给予回复说明，并通过官微进行了公布。北京移动表示，经公司内部查证，获知相关情况如下：2016年4月8日17时54分，手机号码152****1249通过静态密码（客户自设密码）方式，登录北京移动官方网站，经网站弹屏二次确认后，办理“中广财经半年包”业务，IP地址显示登录地点为海南海口；18时13分，手机号码152****1249以同样方式登录网站办理更换4G USIM卡业务。系统向客户本机下发换卡二次确认验证码（6位USIM验证码），该验证码被输入后，换卡成功。前后过程仅用了19分钟。

北京移动指出，以上业务办理流程正常。公司将积极配合有关部门，提供相关证据，进行后续查证。

事件发生后，支付宝的相关人士表示在跟进中。根据事主写到的，支付宝目前已经赔付一笔在支付宝上非用户本人操作的充值行为以及非本人操作转账行为带来的手续费。另外，支付宝已经承诺在事主提交相关材料，并且在保险公司审核后，有可能会全款赔付。此外，百度钱包也表示在跟进中。

专家说

机主实际上配合别人完成远程“补卡操作”

专业人士分析认为，上述案例信息中提及的“USIM卡验证码”是整个事件的关键之一。

“为什么犯罪分子首先要设置圈套，骗取用户的验证码。”

移动安全专家李铁军告诉记者，从客观效果来看，机主相当于配合“别人”完成了补卡操作。

李铁军说，不法分子很有可能利用非正规途径获得的空白USIM，在案件中通过改号软件，伪造了一条短信发到受害人手机上，进而骗取获得了用户的真实验证码，之后换卡“成功”。“当然案例中还有一些情况目前交代不是很清楚，需要公安机关的进一步调查。”

诈骗实施前网友个人信息可能已泄露

此外，攻击者为什么能在很短的时间内完成盗窃，用户对于互联网的各种服务有足够了解度和经验的前提下，他的防护速度仍然跟不上攻击者的进程，李铁军认为这说明攻击者提前已经有足够的准备，提前掌握了一定的用户信息。

据专家分析，按照受害人目前的描述，判断这是一起典型的综合利用“个人信息+ USIM补换卡+改号软件发送诈骗短信”的电信诈骗案件。根据百度钱包的关联来看，很有可能在诈骗实施之前，骗子已经获取了受害人的银行卡号、身份证号、姓名、手机号等个人信息。在这种情况下，骗子只需要得到受害人的短信验证码，即可进行包括网银、支付宝、百度钱包的所有转账操作。于是，骗子选择利用移动的USIM补换卡业务，直接窃取用户的手机卡。

任何时候都不要把验证码给别人

李铁军指出，任何时候不要把自己的验证码给其他人，其中尤其是收到与银行、支付系统以及个人账户有关的短信，一定要确认自己把全部短信内容完整看完，切忌匆忙处理，更要避免贸然把验证码误发给别人。

此外李铁军建议，作为防范，每个人都应提前做好一些应急预案。比如一旦发生手机突然失效，必要时第一要冻结银行卡，冻结第三方支付账号，这些只要借一部手机就可以完成。 ■来源：北京青年报

关注三湘都市报微信看E报。