被骗后『自学』诈骗 背着『伪基站』乱转

近日落网，涉案金额高达七万余元

石家庄一男子因为接收到诈骗短信银行卡被盗刷，因此网上“自学”多半年骗术，在石家庄成了一名“背包客”，这个背包里装着伪基站，散布关于“和校园”的诈骗短信，捕获信息成功后，利用快捷支付从网上购买黄金、名酒等物品变现，最终被裕华分局槐底刑警队抓获，从男子家中缴获作案手机20余部，伪基站部件，以及部分未出售的黄金和名酒，涉案金额高达7万余元。

本报记者 刘涛 文/图


伪基站的部件

1 银行卡被盗刷毫无知觉

今年9月份，省会市民王先生在超市购物，因为现金不够，因此就拿出自己存有17000元的银行卡准备刷卡，可是当自己刷卡时，发现自己的卡上一分钱都没有了。王先生根本想不起自己什么时候刷走了卡上的钱，回去问自己的爱人，爱人也表示根本没有用该卡上的钱。接着王先生通过网上查询，发现自己卡里的钱从网上购买了很多黄金，但是自己从来都没有买过，王先生判断自己的银行卡肯定是被盗刷了。

随后便来到公安机关报警，报警时王先生仔细回忆，自己最近没有丢失过这张银行卡，也没有向任何人透漏过什么信息，为什么会被盗刷，通过警方的提示，王先生才发现自己接到过孩子“和校园”的信息，让下载一个APP，通过警方的调查发现，这个APP正是让王先生中招的木马程序。

无独有偶，10月份省会韩女士正在工作时，接到了某网上商城的客服电话，电话里称：“您好，请问你是否从我商城网上购买了黄金等产品？”韩女士以为是骗子就挂断了电话，紧接着对方又打来电话，韩女士表示自己并没有买，而且对方说出的地址根本不是自己家的地址。对方客服赶紧提示韩女士查询一下银行账户是否被盗刷，韩女士通过查询才发现自己确实被盗刷了近两万元。随后，韩女士赶紧来到公安机关报警，警方通过调查发现，韩女士和王先生的遭遇一样，都是先接到了一条关于“和校园”的短信，然后下载了APP，最终被盗刷银行卡。


部分赃物

2 嫌疑人是人群中的“背包客”

自今年9月份，裕华分局槐底刑警队接连接到市民报案，银行卡无缘无故被盗刷。裕华分局接到报案后立即成立专案组，对案件进行分析研判，通过大量的摸排和走访，初步掌握了犯罪嫌疑人赵某的信息，警方介绍，赵某将伪基站装在黑色的双肩包里，然后在人多的地方发送信息，在一定范围内就有很多市民收到短信，接下来就很有可能被盗刷银行卡，因为嫌疑人作案手法隐蔽，在人群中很难判断。

警方通过大量的走访和巡逻，最终得到信息，得知嫌疑人11月22日将在裕华区某小区出现。11月22日，警方迅速出击，在裕华区某小区将犯罪嫌疑人赵某抓获，并且在赵某的家中起获了伪基站、20余部手机、笔记本电脑等作案工具和部分未出售的黄金和名酒。犯罪嫌疑人赵某对通过伪基站进行诈骗的犯罪事实供认不讳。12月19日，记者在槐底刑警队见到警方起获的伪基站、名酒以及一些嫌疑人未出售的黄金，警方指着伪基站介绍，就是这些东西让很多市民不知不觉地一步步进入圈套，然后银行卡就被盗刷。

3 被骗后网上“自学”骗术

犯罪嫌疑人赵某交代，自己只有初中文化，曾经银行卡也被用同样的手段盗刷，但是赵某并没有报警，自己反而觉得这种骗术简直太高明了，于是就开始从网上搜索资料学习，直到自己加入了“高手群”，然后通过在群里的交流，赵某掌握了核心技能。今年9月份，赵某花费5000元购买了一套用于发送短信的伪基站，又花费800元左右购买了木马病毒并租赁了临时网络服务器。然后根据学习到的知识编写了植入木马链接关于“和校园”升级的相关信息。然后赵某将伪基站放入双肩包中，背着伪基站到人流量较大的场所随机发送短信。据赵某交代，在一定范围内只要打开手机的人都可以收到这条短信。记者也在裕华分局槐底刑警队见到了伪基站，一个主机，两块电池，和一个屏蔽器，构造非常简单。

收到短信的市民会看到“和校园即将升级请点击此链接下载最新的APP……”当有市民下载APP后，按照要求填写自己的身份证号、手机号、姓名等信息。填写信息提交后赵某预先设定好的电子邮箱中就会出现这些信息，这样赵某就成功地收到了受害人的相关信息，下载这款木马APP以后，受害者的短信功能就会被屏蔽，接受到的所有短信都会被赵某窃取，全部会发送到赵某提前输入好的手机号码上，更可怕的是，受害人手机中所有历史短信也同时会发送到赵某的手机或者邮箱中。

赵某再通过筛选含有银行账号的相关重要信息，这样赵某就掌握了受害人的姓名、身份证信息、手机号、银行卡等重要信息。有了这些信息，赵某便可以在网站上购买各种商品，最简单便捷的支付就是手机支付，通过手机支付根本不用密码，只要收到验证码就可以购买，支付的时候受害人的短信功能已经被屏蔽，因此验证码自然就发送到赵某预先设定好的手机上，赵某便可成功付款。

为便于变现，赵某大都选择购买金条、金元宝、名酒等，收到货后将其低价卖到黄金回收摊位获利。

目前，赵某因涉嫌电信诈骗已被刑事拘留，案件正在进一步审理中。

4 “背包客”一秒可发上万垃圾短信

就伪基站问题记者采访到石家庄市无线电管理局监督检查科科长王勇，王勇介绍，“背包客”的设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备搜取100~200m范围内的手机SIM卡信息，然后群发诈骗信息、广告信息或者其他信息。不法分子只需要获取板卡和芯片，就能组装伪基站，成本不高，而“背包客”发送广告短信，量大收益大，“理论上伪基站一秒可发200多条信息，一部机器一天发送几万条信息不成问题。”

这样的伪基站可以随意在收件人手机上显示号码，可以是你的父母子女、老公老婆、亲朋好友的电话，也可以是10086、95555甚至110、120。不过，为了方便实施下一步诈骗，骗子一般会输入银行、运营商等公信力较强的服务号码。并且收件人手机上的内容也可以随意填写，不过，骗子一般会在短信里植入一个网址链接，诱惑你点击，以方便下一步实施诈骗。由于这些号码显示的就是运营商和银行的电话，积分兑换、个人信息核实的理由还说得过去，再加上现在手机上网又是那么方便，所以不少人便会点开其中的网址链接。

王勇表示，伪基站不只是以背包客的形式出现，还可以放在电动三轮车、汽车里、也可以用电动车、摩托车等，所以市民一旦发现应该立即报警，石家庄无线电管理局会及时配合公安部门发现一起打击一起，绝不放过。

同时警方提醒广大市民，只要短信遇到链接千万不要轻易点开，赵某正是利用了家中的孩子在上学，利用家长的心理才使家长们下载APP，因此遇到类似有链接的短信一定要核实后再打开，尽量做到直接删除不要打开。