网购上千银行卡密码,九成正确 五个方法教您防盗刷

60岁的吴先生平常不太会用智能手机,手机中没有网银、支付宝等客户端,即便手机中毒,银行密码也不会泄露,而银行卡也一直在他自己身上,密码也只有他自己知道。可是,他无意中点开了短信中的一张图,卡上的5万元存款一周只剩300元。

银行卡在身,5万元存款一周只剩300元

去年12月,吴先生收到了一条陌生号码发来的短信。短信上写着自己的名字,吴先生以为是某个没存号码的朋友发来的,就点击了短信中的图片。由于手机并未出现什么异常,吴先生便没太在意。可一个星期之后,银行突然发来一条消费短信,原本存有5万多块钱的一张银行卡,余额竟然只剩下300多块钱了。

吴先生查询发现,在这一个星期里他的银行卡陆续在往外转钱,但银行发来的十几条消费短信,他一条也没接到。吴先生把手机拿到客服检查,被告知他的手机中了木马病毒,在一个星期内丧失了接收短信的功能,一个星期后木马病毒失效,短信功能才恢复。

60岁的吴先生平常就不太会用智能手机,手机中没有网银、支付宝等客户端,所以即便手机中毒,银行密码也不会泄露。而银行卡也一直在他自己身上,密码也只有他自己知道。

爆料可网购银行卡密码

就在吴先生案发不久,记者接到了一位自称老徐的爆料人的举报。老徐说,在网络空间存在着一个规模庞大的盗取银行卡信息的黑色产业链。吴先生匪夷所思的遭遇,在他看来只是小菜一碟。“像老吴这种信息在黑市里很容易搞到,我用5分钟就能搞到1000个这种信息,包括卡主的姓名、卡号、身份证、电话号码,还有他的银行卡密码。”

为了验证自己所言不虚,老徐打开了几个QQ群。不到5分钟,他发给了记者一份长达33页的文件,有1000多条银行卡信息,每条都有卡主姓名、卡号、身份证号、银行预留手机号码以及银行卡密码。记者在文件中随机选取了七十个不同省份的信息进行验证。其中,身份信息和电话号码全部正确,除了5个银行卡密码错误,其余65个银行卡密码全都正确。

揭秘盗取银行卡信息三大方法

方法一:伪基站发送钓鱼短信

被盗刷银行卡的受害者大都有过相同的遭遇,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。

反诈骗专家裴智勇指出,这些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。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。

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,记者发现犯罪分子还会利用免费WIFI窃取个人信息。裴智勇介绍,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

犯罪分子利用改装的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。

预防为主,消除隐患 减少损失

1.把磁条卡更换成IC芯片卡

专家表示,磁条卡由于技术问题,容易被不法分子复制,IC芯片卡却不容易被复制。

2.网上交易设定限值

专家建议大家把线上交易的额度做一个设定,避免大额损失。同时,单独申请一张银行卡用于绑定交易。另外,消费者在使用银行卡时,若不能确定用卡环境是否安全,应尽快向银行求助,请银行帮助处理并消除风险。

3.安装安全防护软件

手机安全软件既可防御病毒、木马的攻击,还可以帮助持卡人识别一些欺诈电话、短信等。

4.花小钱解大难

银联方面建议,可购买盗刷险来减少损失。

5.上官方网站查询金融机构真伪

收到来路不明的短信,或有不明的金融机构难以判断真伪时,可以通过上海日前成立的互联网金融信息查询系统进行免费查询核实,避免被虚假、非法的金融机构盗骗信息或资金。

发现银行卡被盗刷 你该这么做

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,而其他地方发生的交易均为伪卡。

■来源于微信公众号中国经济网 微信号 ourcecn

关注三湘都市报微信 看E报。