手机“失守”绑定银行卡成黑客“提款卡”

近日成都市民冯小姐手机收到验证码短信后,瞬间被转走 987 元。银行卡在身上,绑定的手机收到的动态验证码也未曾透露,为何钱还是不翼而飞?记者发现,手机上保留的银行账号信息可能泄露,加上短信拦截手机验证码,网银就可能被攻陷。

手机,如果不善加利用,就不再是手机,而是手雷——这是 2003 年电影《手机》的经典台词,当年是因担心小三短信泄露,10 年后,手机再成手雷。

节前多家媒体报道,因手机卡被人异地补办,通过手机银行转账,最高损失 26 万元。近日《华西都市报》记者也接到热线报料,成都市民冯小姐手机收到验证码短信后,瞬间被转走 987 元。

让冯小姐不解的是,银行卡仍在身上,和银行卡绑定的联通手机收到的动态验证码也未曾透露,为何钱还是不翼而飞?问题到底出在哪?

A 讲述“什么都没做,钱没了”

8 月 12 日早上 7 点,成都市民冯小姐仍在睡梦中,手机短信响起。银行消费 987 元的“验证码”短信,让她彻底没了睡意。谨慎的她意识到银行卡可能出了问题,连忙打电话到银行挂失,但仅一分钟时间,这 987 元被蹊跷转走。挂失之后,她又收到几笔“验证码”短信……

近日,记者见到冯小姐,她正在去往银行的路上,脸上写满了焦虑和疑惑。

“我啥子都没做,还在睡觉呢,钱就没了。”冯小姐连忙掏出手机,给记者看手机收到的一系列短信。

在事发当天早上 7 点多,冯小姐连续收到好几条验证码短信,一条“末位 3014 的订单,需要支付 987 元”的验证码短信,还有三条“购买北京乐和彩每笔 500 元”的验证码短信。

“收到第一条短信,我就觉得不对,卡在身上,也没有用网上银行,连忙打电话给银行客服挂失。”冯小姐说,一分钟的时间里,987 元已被刷走。

而后面几笔 500 元,因为挂失及时,并没有造成损失。这一分钟,让冯小姐心跳个不停。“挂失慢点的话,不晓得有好惨!”

987 元被离奇转走,让冯小姐觉得银行卡不再安全,当天她就来到银行解挂,并把卡里的 7 万多元都取了出来。

查询这笔钱的走向,发现 987 元被打入一家“浙江贝付科技”的第三方支付公司。

事后,冯小姐第一时间前往成都春熙路派出所报警。据冯小姐介绍,派出所告诉她,像这样报案已经接到好几起,涉案的不少是贝付科技。

浙江贝付科技到底是家什么公司?记者百度查询发现,该公司是一个支付服务提供商,总部在杭州,可以提供在线支付、移动电话支付和货币兑换。

《华西都市报》记者拨通了浙江贝付科技的客服电话,对方告诉记者,七八月确实接到不少来自成都地区的投诉,但贝付科技也只是一个中转渠道,不排除犯罪分子在贝付科技上开账,取到钱后再提现到自己银行卡上的可能。“我们要取得全部订单号,才能查到资金的流向。”

B 疑惑动态验证码不安全?

那么,冯小姐及其他受害者的钱到底是怎么被转走的呢?

据冯小姐回忆,她没有办理网银、网银盾和电子口令卡,只办理了短信通知服务。但 8 月 13 日中午,冯小姐再次前往银行。经过查询发现,签约银行卡时,网银功能已被开启。也就是说,冯小姐的银行卡安全保障只能是“登录密码+手机动态验证码”这种方式。

事后冯小姐登录网银后发现,上面已经有了 5 次登录记录。冯小姐的账号和密码已经被攻陷。但是犯罪分子又是如何获得冯小姐的手机动态验证码的呢?

C 分析安卓系统更容易中招

面对这样一种网银蹊跷消费的情况,四川省公安厅刑侦局相关负责人接受《华西都市报》记者采访时分析,犯罪分子要转走冯小姐的钱,一是要获得冯小姐的卡号和网银登录密码,二是手机被黑客攻克,收到的手机动态验证码被拦截。犯罪分子获得卡号与网银登录密码,有两种渠道,一是在受害者电脑上植入木马,盗取这些信息。二是受害者在线下 POS 机上刷卡消费,也有可能泄露卡号与取款密码。

“鉴于冯小姐没有使用过网银,我认为是冯小姐在刷 POS 机时不小心信息泄露。”该负责人表示。

而犯罪分子又是如何看到冯小姐的手机验证码呢?

冯小姐使用的是安卓系统,金山安全专家李铁军告诉记者,在安卓开放系统下,黑客是有可能拦截到短信的。“有一种恶意软件,只要手机安装了,收到的短信就能自动转发到指定手机,或上传到服务器,黑客就能实时看到短信内容”。还有一种黑客软件,受害者收不到短信,而黑客能收到,这样受害者不会产生警惕挂失,只有查账时才知道钱被转走。

李铁军表示,安卓手机容易中招,因为它能从各种渠道下载应用,给黑客可乘之机,“比如刷了恶意二维码”。

而苹果 iPhone 只能通过 ppStore 下载应用,一般情况下有一定的安全保障。

延伸阅读

“补卡攻击”让手机变“手雷”

据《阳光报》报道,陕西宝鸡陈先生 9 月 21 日手机接听突然掉线,4 分钟后银行账户内 26.8 万元被人转走。事后调查,原来是手机卡在位于成都的营业厅被办理补卡,被人以手机银行转账的形式,分三次转入一个陌生账号。

无独有偶,据《长沙晚报》报道,9 月 26 日,长沙市民黄先生的手机卡,被人在成都营业厅补办,结果有 12 万余元存款的银行账户只剩下 500 余元。

同样是在 9 月 26 日这一天,据《新京报》报道,北京袁先生的联通手机卡也在异地被重新制作、补办,工资卡里 10.9 万元存款,只剩下 700 余元。

《华西都市报》记者发现,腾讯 QQ 安全中心、金山毒霸等官微均就上述案例发出警报,称这是“补卡攻击”。

认证为“腾讯安全平台部部门负责人”的 coolc 称,这种攻击常见手法为利用二三线城市的运营商营业管理松散问题补办卡。一旦犯罪分子补办了 SIM 卡,就可以轻松获取手机动态验证码,将手机银行资金转出。

据《长沙晚报》报道,在已破获的一起案件中,警方发现,2013 年以来,犯罪嫌疑人陈某通过非法渠道获取他人的网上银行账号及个人信息,首先办理假身份证和驾驶证,到运营商营业厅补办受害人的手机卡,再通过网上银行,将受害人银行账户内的钱盗窃一空。

运营商说法

补卡除了身份证还需电话联系记录

如何避免假身份证补办 SIM 卡?记者采访了四川三大运营商。四川移动相关负责人表示,中国移动的许多业务,像补卡等都需要身份证和服务密码才能办理。记者致电移动客服如何补卡时,也印证了上述说法,必须提供身份证和服务密码,如果忘记服务密码,还需提供最近 5 次电话联系记录。

四川联通相关负责人表示,补办卡业务,必须本人持有效身份证件并提供给服务密码到营业厅。不过,当记者致电联通客服时,客服告诉记者如果是机主本人持身份证原件补办手机卡,无需提供服务密码。

四川电信相关负责人接受采访时称,电信对补办手机卡有一套严格的程序,需要本人持有身份证原件到营业厅才能补办。

安全揭示

“密码+手机动态验证码”并非绝对安全

据上市银行半年报显示,今年上半年,国内 9 家银行手机银行的累计用户数量已经超过了 3.4 亿。怎样才能让手机银行和手机绑定的网络支付更加安全?

专家建议,用户要提高安全防范意识,不要认为单凭有密码和手机动态验证码就是绝对安全的。在通过手机绑定的网络支付时,最好还要有多重防护,比如办理网银盾、电子口令卡等再次保障安全的工具。

涉及网络支付时,一定要选择正规电商网站进行交易,安装专业的手机安全软件,查杀和拦截手机盗号病毒,并识别短信、网页中可能存在的“钓鱼”网站链接。

另外,要妥善保管好手机和密码、设置合理的转账支付限额、开通及时短信通知服务、提防虚假 WAP 网址和网络钓鱼、使用完手机银行后应及时清除手机内存中临时存储账户、密码等敏感信息等。

使用手机银行的用户,在碰到不能收发短信,或者无法接打电话时,也一定要多一个心眼,及时关注 SIM 卡是否被补办,以及手机银行的资金动向。

而银行如何及时针对新型犯罪手段,设置更加让人放心的支付、转账保密程序,也成为消费者关心的问题。

(据《华西都市报》)