

“被消费”“被贷款”……

手机失窃遭“盗刷”暴露哪些安全漏洞

近来,一篇网络文章受广泛关注:一名网友叙述了家人手机遭盗窃后“被消费”“被贷款”的遭遇。文章引发公众对手机失窃可能带来的财产安全问题的担忧。

目前,大部分涉事支付机构已赔付受害人经济损失。工业和信息化部也于日前约谈涉事电信企业相关负责人,并提出对于服务密码重置、解挂等涉及用户身份的敏感环节,要在方便用户办理业务的同时强化安全防护。

记者发现,虽然这是一起偶发事件,但暴露出一系列涉及公民个人信息和财产安全的漏洞。

手机失窃被不法分子进行多笔消费和贷款

据网民“信息安全老骆驼”称,其家人手机失窃后,不法分子利用电信、金融、支付等机构以及互联网金融平台的安全漏洞,新建账户绑定银行卡,几个小时内,便在线办理了贷款,并进行多笔消费。

不法分子是如何利用手机盗取资金的? “信息安全老骆驼”向记者复盘了遭遇“盗刷”的全过程:不法分子取出机主手机卡,将之安装在自己的手机上,通过短信校验的方式,登录了某政务平台App,由此获取了机主的姓名、身份证号、银行卡号等关键个人信息。通过这些关键信息及校验短信,进行服务密码重置,掌

握了对手机卡的主动控制权。此后,在支付宝、财付通、苏宁易购、京东支付等开立了新账户,绑定机主的银行卡进行消费,并在美团平台申请贷款,造成机主经济损失。

整个过程中,登录政务平台App获取关键信息、绑定银行卡、贷款消费等操作,都是凭借手机短信验证码顺利通关。

记者了解到,此案之所以产生如此后果的一个重要原因,在于手机遭窃后机主没有第一时间挂失电话卡,令不法分子有了可乘之机。

专家解释,在电话卡未挂失的近2个小时,由于掌握了机主个人关键信息,不法分子通过手机在线服务,对服务密码进行了重置。这相当于掌握了通信业务办理的主动权,能进行远程解除挂失,还可以利用短信验证码登录其他网站和App。

手机信息和支付安全漏洞引发多方担忧

这一网民的遭遇暴露出手机信息安全和支付安全的多个漏洞,引发多方担忧。

——电话卡解除挂失等安全机制有待升级。

据其本人介绍,案发当日,在通过电信客服挂失后不久,他们发现手机卡居然被不法分子解除挂失,仍能使用。双方进行了激烈斗争:挂失、解挂、再挂失、再解挂……来来回回几十

次。其间,这张手机卡不断接收消费和贷款的验证短信。

多位业内人士表示,虽然机主手机被盗后未及时挂失电话卡,让不法分子钻了空子,但电信企业的服务密码重置和解挂失等业务规则是否完善、是否充分考虑了机主手机丢失的可能性,值得探讨。

按照中国电信的业务规则,已挂失账户可以通过拨打客服热线、服务密码鉴权后进行解挂。利用机主挂失前的“空档”,不法分子通过机主姓名、身份证号、短信随机码重置了服务密码,掌握了通信业务办理权,多次诱导电信企业客服人员为已挂失的电话卡进行解挂。

电信专家付亮认为,用户反复解除挂失的异常举动,应及时引起电信企业包括客服人员在内的系统的警觉,适当升级安全门槛,而不是依然机械地进行常规操作。

——校验手段普遍不足,风控水平参差不齐。

目前,虽然监管部门对于支付机构开户身份的安全验证有相关规定,但部分机构执行打了折扣。

记者调查发现,不少金融平台和支付机构开立账户或绑定银行卡的流程较为简单,一些机构在授信流程中,只增加了银行短信校验或者公安网校验,就顺利放款。在此案中,不法分子通过机主的银行卡号、身份证号、姓名、银行预留手机号等信息,加上短信验证码,就在美团平

台上办理了贷款业务,并很快将贷款通过新开立的支付账户消费掉了。

业内专家表示,为吸引用户,部分金融平台不会在绑卡开户时增加烦琐的校验方式,而是简化开户流程。更有一些小公司,为节省成本而省略步骤,校验的完成度和可靠性难以保障。

与此同时,一些平台和机构风控水平不过硬。从网民“信息安全老骆驼”家人的遭遇来看,同样在凌晨三四点,有的支付系统风控成功识别了异常交易并进行阻断,有的则通过了不法分子的贷款申请,有的支持了不法分子数笔绑卡消费。

——个人敏感信息保护不力。

该案中,不法分子通过短信验证的方式便登录了某政务平台App,获取机主的重要信息如探囊取物一般。

业内专家表示,身份证信息和银行卡信息属于个人敏感信息,一旦泄露后果严重。身份验证要强化甄别“确为本人意愿”,如借助人脸识别等方式提高验证门槛。

此外,一些通信行业人士表示,一些无良手机App过度收集个人信息,也为个人信息安全埋下隐患,一旦App被入侵就会造成严重信息泄露。在公安部组织开展的“净网2019”专项行动中,被查处的违法违规采集个人信息的App就多达683款,其中不乏知名企业。

据新华社



69岁的王远明拿着183万元的存单。

37岁男子婚礼当天坠亡 妻子起诉要求查封财产 69岁公公维权:这183万存款是我的积蓄

“这是我的存单,183万,我和我儿子一块儿存的。当时我没带身份证,写了我儿子的名字。我没想到儿子会去世,会有这个事儿。”

22日,辽宁锦州69岁老人王远明接受记者采访时非常懊悔,经历丧子之痛,如今又面临儿子两任妻子争夺这笔存款,老人心力交瘁。

用儿子名义存了183万 没想到儿子婚礼当天坠亡

“我经商20多年了,这183万存款是我做生意的积蓄。”王远明告诉记者,他在锦州做机电材料生意多年,儿子王亮一直跟着他在店里打工。

“2016年9月16号,到银行存这笔钱时,因为现金金额比较大,我拿着不方便,就喊儿子一起去了。当时走得匆忙忘带身份证,我就用我儿子的名义存的,但密码是我设的,存单也是我拿回来放保险柜里的,上面的指纹手印都是我的,这个手印可以鉴定。”王远明回忆道。

2019年3月8日,离异后的儿子和锦州本地一个80后女子办理结婚登记,两周后的2019年3月23日,正是两人的大喜之日,却发生了令人匪夷所思的事。当天,订的上午11点18分办婚礼,没想到9点27分,王亮从女方家所在小区15层楼高的楼顶坠亡,至今死亡动机都是谜。

据介绍,锦州市公安局太和分局一直没有立案,警方勘察了现场,经过调查没有发现他杀的证据,最后定性为自杀,但并没有为家属出具不立案通知书。王亮没有遗书,生前所用手机被警方带走调查,他的新婚妻子也没有解释,王远明夫妇到现在也不知道儿子为什么会坠亡。

被冻结的存单 两任妻子起诉要查封财产

王远明今年69岁,老伴67岁,就王亮一根独苗。王亮去世时才37岁,没等老人从失子之痛的打击中缓过神来,王亮的两任妻子竟然都要分割183万元存款。

“存单是5年定期存款,现在还没到期,要到2021年9月16号才到期。但现在也取不了了,因为儿子的新婚妻子起诉后,这笔存款被法院给冻结了。”王远明告诉记者,儿子突然离世没多久,新婚妻子就去太和区法院起诉,要求查封王亮名下所有财产。

此外,王亮的前妻也提出诉求。现在,王亮的两任妻子都要分割财产,要求对这笔存款主张权利。

王远明表示,这笔钱是自己做生意的毕生积蓄。儿子当时一个月才3000多元收入,是不

可能有183万元存款的。

“存款是我做生意的积蓄 和她俩没关系”

王远明断断续续地介绍,儿子和前妻是在2016年12月离的婚,“他们开始还瞒着我,我不知道他俩离婚了。”

“这笔存款其实和她没有一点关系。因为她生了我孙子,我儿子去世后,她帮着料理后事,我挺感动的,我听说她每月要打好几个工,就让我妻子每月给她500元,还给了她32.5万元,她说要给我孙子买房子,其中包括替她还了9.6万元的路虎车贷。”

王远明表示,儿子和现任妻子是2018年认识的,“这笔存款和她半毛钱关系都没有。”就因为当时用儿子的身份证存钱,才惹出后面这一系列事情。

王远明表示:“谁会想到会出这个事情,我现在心里不服,我是光明正大的,银行也能证明存款是我的。”

22日,记者联系王亮的现任妻子,她表示应该去司法机关了解情况。“我是一切听法院的,国家有规定,法律有条文。法院怎么判,我怎么接受。” 据《华商报》

没完没了 证明“我爸是我爸”咋就这么难?

近日,广东惠州的陈先生在国务院“互联网+督查”平台上反映了一件烦心事:为了继承已故父亲的一笔存款,需要办理公证,但陈先生在银行、公证处、派出所、居委会来回跑了7、8次,历时7个多月,还是没能拿到他父亲的存款。

“循环证明”没完没了

陈先生父亲于今年2月28日去世,去世前在中国邮政储蓄银行惠州支行留下7万余元存款,3月2日,陈先生拿着存单(知道父亲存单密码)去银行取款时,由于不能通过银行人脸识别系统,取款没有成功。

银行工作人员告诉陈先生,他这种情况属于存款继承,应向本人住所地、经常居住地或银行机构所在地的公证机构申请办理继承权证明书,银行凭此支付。就此,陈先生踏上了办理继承公证、证明“我爸是我爸”的漫长循环。

此后大半年里,陈先生为此事又多次奔波于银行、公证处、派出所和居委会之间,但问题迟迟解决不了,陈先生仍然未能办下公证书,导致银行存款无法取出。

督查组督查整改“循环证明”

国务院第七次大督查第十一督查组接到陈

先生反映的问题后,赴广东惠州实地督查,走访了银行、公证处、派出所、居委会等单位,发现问题属实,向陈先生所在的惠州市惠阳区政府反映该问题,惠阳区政府立即召开协调会研究整改措施。经协调,陈先生父亲原所在单位同意出具亲属关系证明,10月20日,陈先生的公证手续已办完,继承的存款也已从银行取到。

此外,为杜绝类似问题再次发生,惠州市已要求惠阳区对相关办理流程进一步优化,为确保公证事项的真实性和公安户籍数据的安全性,类似事项的办理,由区公证处发函至区公安分局,区公安分局出具亲属关系证明,为群众提供更加便捷高效的服务。接下来,惠州市将在

全市举一反三,对类似问题进行梳理和排查,督促问题全面整改到位。 央视

版权所有 违者必究

总值班:贾敬伟
一版编辑:吴天奇
一版美编:王晨同

零售
专供报



619359701566666