



一部手机失窃遭“盗刷”引发的担忧

网民的遭遇暴露出手机信息安全和支付安全的多个漏洞

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。

据了解，案件正在进一步调查中。

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登录其他网站和 App。

被“盗刷”暴露出哪些安全漏洞

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对其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，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，一旦遭泄露后果严重。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 被侵入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。

机构与平台应提高安全验证手段

事件曝光后，大部分涉事的平台和支付机构消除了受害人的贷款记录，并赔付了损失。记者了解到，相关支付机构已着手加强手机丢失防控策略，提升风控水平，适时升级身份验证手段。

针对电信企业存在的漏洞，工业和信息化部日前约谈了此次涉事电信企业相关负责人，并对三家基础电信企业提出要求，对于服务密码重置、解挂等涉及用户身份的敏感环节，在方便用户办理业务的同时要强化安全防护，加强客服人员风险防范意识培训，警惕业务异常办理行为。

中国电信相关人员表示，为进一步防范此类风险，将强化和规范挂失、解挂、呼转等业务的鉴权方式和流程，增加技术核验手段，提高服务人员风险防范意识，对频繁办理业务的行为加强监控，对异常行为进行限制和升级操作授权。

“无论是支付业务还是其他金融业务，都应该把安全性放在第一位，其次才是便捷性。”国家金融与发展实验室特聘研究员董希淼表示，非银支付机构及互联网金融公司担负着数以亿计用户的财产安全，有责任不断加强风险防控。针对手机失窃这种情况，金融机构应该考虑得更全面些，不光要“实名认证”更要“实人认证”。

此外，付亮说，相关单位和企业应及时对用户数据进行脱敏处理，按照最小必要原则收集、存储、使用，并注意分级分类保存。

普通民众如果手机被盗或遗失，应如何保护个人信息和财产安全？

专家提示：

第一时间致电手机运营商挂失 SIM 卡，以免不法分子利用“时间差”窃取个人信息。

尽快致电银行冻结手机网银，只要办过银行卡的银行都要覆盖到，不要给不法分子留下可乘之机。

对支付宝、微信等具有金融功能的应用及时进行冻结，且密切关注账户服务和资金变动。

通知亲朋好友手机遗失，让他们不要轻信陌生人打来的电话或发来的信息。如果发现异常的资金使用情况，及时拨打 110 报警电话报案。

据新华社



■手机失窃后，支付宝账号遭登录、“被消费”。