支付宝曝重大安全漏洞 熟人能轻易盗号刷走你的钱?

公司回应:已提高安全等级;记者实验:修复后想盗很难,即使登上账号也支付不了

1月10日凌晨,有网友在微博爆料称,支付宝登录出现安全漏洞,有网友表示,只要登录他人的支付宝账号,选择"忘记密码",就可以通过安全问题验证(识别近期购买物品或好友)找回密码,从而登录别人的支付宝账号。

此事一出,不少网友纷纷亲身尝试之后将自己的实验结果发布在微博和朋友圈里,不少网友怀疑:"由此产生的熟人盗窃怎么办?""十几年的用户积累,毁于这个致命漏洞",一时间,朋友圈里都被"支付宝致命漏洞,快解绑你的银行卡"刷屏。

支付宝真的有安全漏洞吗?现代快报记者进行了实验求证。

现代快报/ZAKER南京记者 王静 丁晟

实验一 按照网传方法能成功登录账号

按照在网络上传播的步骤,1月10日中午12点左右,现代快报记者尝试在自己的另一台手机上登录支付宝账号。记者点击忘记密码后,跳出的是"输入验证码"的一个界面。

几乎与该界面跳出的时间同时,账号绑定的手机号码就收到了短信验证码的短信提醒:千万不要把验证码告诉别人。

现代快报记者发现,这是整个实证过程中,唯一一次收到来自支付宝的提醒,但支付宝除了提醒不要把验证码告诉别人之外,并没有提示有人在其他手机端尝试登录支付宝账号,或者说支付宝账号存在安全风险。

按照网传步骤选择"无法接收验证码"。果然出现了如网上所传的"图片验证题",图片验证题是两道"单选题",第一题是在9张图片中选择最近在淘宝上买过的东西,第二题则是在9张头像中选出自己支付宝好友头像。只要答对这两道题,就可以重新设置密码,并在该手机上登录支付宝了。

而在修改密码和登录的过程中,支付宝账号绑定的手机没有收到任何短信提醒。

实验二 登录账号难度升级 即使登上了也无法支付

但当记者下午3点再次在该手机上退出支付宝账号,尝试重新登录时,按照忘记密码的步骤操作,选择"无法接收验证码"时,原本的"图片验证题"却不见了,转而是要求输入证件号码。

在输入证件号码的下方,有一行蓝字"换个方式找回密码",里面分别有:填写身份证件号、回答安全保护问题、验证已绑定的银行卡信息、刷脸验证、验证本人银行卡信息、拨打验证电话等选项,记者一一实验,验证之后发现,"回答安全保护问题"一项相对容易被"熟人"攻破。

比如问题是"我爸爸的名字是?"如果是发生在熟人之间,其实并不是一个难题。

成功登录之后,现代快报记者尝试转账交易发现,免密支付和指纹支付已经被暂时锁定,只能通过输入交易密码,完成交易后才能再次开通这两项功能。而如果选择忘记交易密码时,则需要通过更严格的"验证银行卡信息"以确认为本人操作。

实验三 陌生手机无法使用安全问题验证

在前两次的实验当中,现代快报记者发现,只要点击"忘记密码",在跳转页面时就会出现"正在进行智能安全检测"的字样。

支付宝又是怎样判断尝试登录操作的手机是否安全呢?

现代快报记者又换了另一部从来没有登录过该账号的手机。第一次,记者正常输入密码登录,并完成了一笔转账交易后退出登录。模拟了一个借熟人手机使用支付宝的场景。将手机还给熟人之后,对方能够登录上去吗?

还是用同样的步骤,但当记者点到"换个方式找回密码"时,"图片验证题"和"回答安全保护问题"都没有出现,而是直接跳出绑定银行卡的选项,如果不能绑定银行卡,则没有办法登录支付宝账户。

网传的支付宝账号破解方法:登录手机账号——忘记密码——手机不在身边——淘宝买过的东西9张图片选1个——好友验证,9个好友图片选1个——修改密码——登录成功

支付宝回应

安全问题验证 仅能在本人手机使用

针对网友的担心,支付宝昨天也做了回应。支付宝工作人员告诉现代快报记者:"通常情况下,用户找回登录密码至少需要输入手机短信验证码,只有对于部分暂时无法收到短信的用户或者更换移动设备的用户,风控系统才会先进行评估(比如账户信息完整程度、网络环境等因素),并在安全系数较高的情况下,才让用户回答一系列安全问题,而且只有在回答正确后,才能修改登录密码。另外,即便账户被别人登录了,账户的钱也不会被轻易盗走,转账或购物进行支付操作都得输入支付密码。支付密码的修改难度很大。"

支付宝同时表示,已经于10日上午进一步提高了风控系统的安全等级。目前,仅在用户自己的手机上,才能通过识别近期购买商品以及识别本人好友来找回登录密码,通过其他手机设备是无法应用这一方式找回登录密码的。

专家提醒

发现账号异常 应及时挂失

有安全专家还提醒,目前,很多人习惯丢失银行卡、手机后及时挂失。随着移动互联时代的到来,很多人的生活已与网络账户息息相关,网友们也应当建立起给网络账户挂失的习惯,当手机丢失,不仅需要给手机号码挂失,也需要对手机绑定的网络账户挂失。

例如,如果用户突然收到支付宝发来的验证码短信,说明有人尝试登录支付宝账号,可以立刻进入支付宝客户端,进入安全中心快速挂失或拨打支付宝服务热线95188挂失。

融360理财分析师肖微微还提醒,如果手机突然间收到大量的验证码,这种情况可能是不法分子故意发送的垃圾短信,意图掩盖修改密码或解绑手机等安全提醒类短信,这种情况此前已经有发生,如果发现,大家也需要留心。

安全贴士

前期多做安全准备 防患于未然

用户在享受移动支付的便捷性时如何提高安全性呢?融360理财分析师肖微微告诉现代快报记者,做好几项预防工作可以有效阻拦安全风险。

1 设置多重密码保护

移动支付已经较为普及的今天,支付账户安全性的加强首先是要设置多重密码进行保护,包括设置手机开机密码(锁屏密码),支付账户登录密码和支付密码,这些密码最好设置成互不重复且非常规的密码(免得被轻易猜出)。

2 提升安全问题难度

一般账户登录密码找回可以通过回答安全问题,或其他方式与回答安全问题组合来找回,所以用户还需要提升安全问题的难度。系统验证是匹配问题与答案是否对应,所以不用拘泥于答案的真实性,设置你能够记住的非常规答案最好。

3 主动调低信用额度

对于一些有信用额度的账户而言,即使账户内没有现金,也要注意有信用额度被盗用的可能,比如支付宝的花呗、借呗等信用产品,微信微粒贷等。主动调低信用额度,万一账户真的被盗,也能减少财产损失。

4 为支付账户上保险

为账户安全购买保险也是一种积极的办法。比如支付宝的账户安全险,账户资金被盗转等情况可获赔付。这类保险的保费很低,最多不超过2元,但保障额度能达到100万。"但账户被盗的关系人是直系亲属或者夫妻关系的话获得赔偿的概率会比较低。"