

手机支付十大坏习惯 你中招了没



昨日,本报对坊间热传的几种Apple Pay的盗刷方法“见招拆招”,不少果粉仍心有戚戚焉。

这不,就有微博网友爆料,有用户使用Apple Pay绑定信用卡失败后,一小时被盗刷上万元。

当手机成为越来越多市民的“第二钱包”,从出门打车,到超市购物,再到饭店买单等等,几乎涵盖了每天的衣食住行。

但是,手机支付在带来便利的同时,也隐藏着很多安全隐患。本期,我们就一起了解手机支付的十个坏习惯,自测一下你中招了几个?



关注三湘都市报微信看E报。

当手机出现这些情况 你就要小心了!

案例1

手机突然没信号

手机长时间没信号?不要以为只是网络或手机故障,还有可能是面临账户被盗刷的安全风险。

单先生在外出差,突然发现手机没有信号,以为是当地信号不好或手机故障没有在意。当天回到北京后,手机依然没有信号,在询问营业厅后,工作人员称有人给他的号补办了SIM卡,因此他使用的卡已作废。

当单先生查询支付宝账号和捆绑的银行卡时发现,支付宝内65000元及与支付宝捆绑的银行卡内的2000元已被盗刷。

案例2

手机丢失后被人购买

去年7月,喻某购买了一部来历不明的苹果手机,由于未设开机密码,喻某发现该手机里的支付宝App可以直接点击登入,支付宝账号里尚有余额1000余元及绑定的借记卡。

于是他通过手机的设置功能,通过界面把指纹登入改成自己的指纹,利用被盗手机支付宝,扫描充值二维码及指纹支付多次为其网络账号充值虚拟货币,消费了5万余元。

案例3

手机被人“操控”

一个晚上小额支付30多笔,被盗刷9000多元,全是通过手机上多个第三方支付软件完成。福州市民石先生遭遇了新型网银盗刷,他安装在手机上的支付宝、快钱等第三方支付软件,全都被人“操控”了。

更让他心惊的是,被盗刷30多笔,他的手机不仅没收到一条扣款提醒的短信,还疯狂向外发送了800多条短信。运营商表示,这可能是最近才出现的新型网银盗刷,最大可能就是不法分子将病毒植入石先生手机,操控了他装在手机上的多个第三方支付软件。

总结

网络诈骗花招层出不穷,大家一定要时刻提防!养成好的支付习惯,不轻易向外人透露个人信息,更不要随意“扫一扫”;若发现手机中毒,要及时到手机专业售后部门维修;发现资金被盗,更要第一时间报警。

■本报综合

1 无密码 不设手机屏保密码

一旦手机丢失或被盗,手机中的个人信息及隐私必将暴露无遗。

2 旧手机不处理就出售,个人信息会轻易被他人知晓。

注意!

3 跳过软件用手机浏览器购物

在浏览器购物容易出现钓鱼网站,为保险起见,最好到软件中支付购买。

4 淘汰手机不彻底删除私人信息

街头、商品上和买家发来的二维码不可轻易扫,容易泄露信息,尤其不要为了蝇头小利随意“扫一扫”。

5 应用程序退出不彻底

一些支付软件有小额免密功能,若不彻底关闭,手机丢失后易造成损失。

6 见二维码就“扫一扫”

骗子常常利用短信链接传播病毒木马,从而盗取个人信息和资金情况,切勿点击不明链接。

7 蓝牙常开启有隐患

蓝牙可传播病毒,别人通过蓝牙间谍软件可查看你的电话、短信、替你拨号等。

8 随意点击短信链接

最好从正规的应用商店下载,不要看见应用就下。

9 当心! 蹭免费无线WIFI

不少免费的公共WIFI,安装了木马和钓鱼网站,专门盗取个人信息,要小心!

10 下载山寨软件

手机记事本上不要记录重要敏感信息,手机丢失后极易泄露。

11 在手机上存储重要信息