现如今手机支付越来越方便了，人们动动手指随时随地就可购置自己需要的东西。不过手机支付虽然方便，但背后的漏洞也不容忽视，针对近期手机支付被盗刷的情况频发，《警周刊》总结了使用手机支付的九个坏习惯，自测一下看你中招几个？

一、不设手机屏保密码

不少人为了图省事，干脆不设手机密码，这样任何人拿到手机后就能随意查看，毫无隐私。

二、通过手机浏览器购物

在浏览器购物容易出现钓鱼网站。互联网上充斥着各种不安全因素，不法分子可以通过病毒、钓鱼网站等非法手段获取消费者的一些信息，再加上支付过程的极度简化，更容易对消费者的财产造成威胁，市民最好还是软件中支付购买。

三、应用程序退出不彻底

很多市民都以为点击手机的HOME键退出应用程序就可以了，其实这些程序仍旧在后台还在运行，这时如果让不法分子拿到手机，轻轻松松就能套取手机信息。

四、不加辨别蹭免费网络

免费的午餐没那么好吃，公共WiFi常被不法分子移植木马及钓鱼网站，不但安全隐患多，而且容易盗窃手机内的个人信息。

五、蓝牙保持开启状态

通过蓝牙传播病毒的案例宁波比较少见，但广大市民不可不防，因为通过蓝牙间谍软件，不法分子可以查看你的电话本、信息、文件，修改你的音量，替你拨号等，所以平时没有特殊用途时，请及时关闭蓝牙。

六、淘汰手机时不彻底删除私人信息

旧手机不处理就出售，里面的个人信息会被拿到你手机的人知晓。

七、下载山寨软件

看见应用就下是个不好的习惯，最好是选择大型的应用商店下载，否则很容易安装到一些绑定有木马的软件。

八、随意点击手机短信链接

各式各样的诈骗信息让用户防不胜防，有些可以向手机发送欺诈短信，诱使用户安装木马或者登录钓鱼网站，从而获得用户账号密码、资金情况等信息。所以对于活动获奖、邀请你查看相册、提示你密码出现问题等等的链接，还是不要随意去点击，应先想办法核实真实性。

九、见二维码就扫

二维码的背后可能会隐藏病毒、木马，你手机里的个人信息可就很轻易地被别人盗取了。

如何防范这些安全隐患？

1、需要手势密码登录的软件应定期更改手势密码，最好不要用手势密码。

2、关闭小额免密码支付功能，不用密码就能支付，容易被不法分子钻空子。

3、使用数字证书、支付盾、手机动态口令等安全产品。

4、安装软件时确保来源的安全，不点击不明链接，不安装不明软件。

5、如果不是经常使用，平时可以关闭余额支付和移动支付功能。

6、在公众场合最好不要用手机支付，尤其是在公开的wifi环境中。

7、大额支付最好开启短信验证功能。

8、在任何场合都谨慎保管包括身份证、银行卡、手机验证码等隐私信息。