当下，不少人用微信、支付宝绑定了银行卡和信用卡，什么交费、外卖、电影、打车……等等数不清的支付功能都可以用微信和支付宝付款。但手机在提供便利的同时，也暗含很多安全隐患，再图方便省事也不能在手机里保存这些信息。究竟哪些信息最好不要保存在手机里？除此之外还有哪些信息也不能相信？我们又应该如何保护手机账号的安全呢？小圈这就带你去了解一下！

01

哪些信息最好不要保存在手机里？

第一张：身份证正反面照片

手机下载很多软件，个别的都需要进行实名认证，因此我们认真完成以后，这些照片都会保存到我们的手机上面，一般大家都不会及时删除。经常使用支付宝的用户应该知道，我们修改支付密码的时候，选择身份证正面照片和短信验证，就可以成功修改支付密码，这样就会出现盗刷情况，所以身份证照片千万不能保存在手机里面。

第二张：银行卡照片

自从移动支付出现以后，我们很少会使用银行卡，除非去ATM机取现的时候，才会用到银行卡，平常的话我们只需要手机绑定银行卡就可以了。绑定银行卡的时候，只需要卡号和银行预留手机号码就可以绑定成功，如果我们手机丢失以后，刚好手机里面留有银行卡照片，这个时候可能会被不法分子进行盗刷。

第三张：记录账号和密码的照片

很多人由于自己粗心，或者记性不是很好，这个时候就会全部写在一张纸上，然后在用自己的手机进行拍照下来，保存到手机相册里面。虽然手机有锁屏密码，但是对于一些有“技术”的人来说，这都不能阻止他们解开，如果你将微信和支付宝密码以照片的形式保存在手机里面，那后果不堪设想。所以，微信、支付宝上有钱，还都绑定了银行卡或信用卡，最好把手机里面的这三张照片都删除。

02

哪种信息诈骗比较常见？

如果你的微信或支付宝收到【你的微信/支付宝账户尚未二次实名验证】，千万不要点链接进去，二次实名认证是假，骗子想骗钱是真！

目前微信并没有所谓的“二次实名认证”。这是骗子把自己的头像和名称修改伪装成“官方”，再给用户发送钓鱼链接。通过假二次实名验证的链接让用户填写银行卡、密码、短信验证码等信息，诱导用户从银行卡转账，还存在泄漏个人隐私信息等风险。如果，收到一条“陌生号码”发来的短信，你可能会直接忽略或者删掉。可如果短信中出现你和你朋友的名字，出于好奇你肯定会点开看~~而就是这么一“点”，你的银行卡可能都不再“属于”你了！

相信很多人都收到过各种诈骗短信，经过梳理发现，此类短信最常见的有这样几大类：

1、看看我们之前的回忆影集，或者这是上次聚会的照片，好珍贵的留影，你快看看吧。

2、请打开查阅你孩子近期在校综合评定成绩并指导，祝你生活愉快（附链接）。

3、这是你于某日某月某地交通违法记录，请查看。

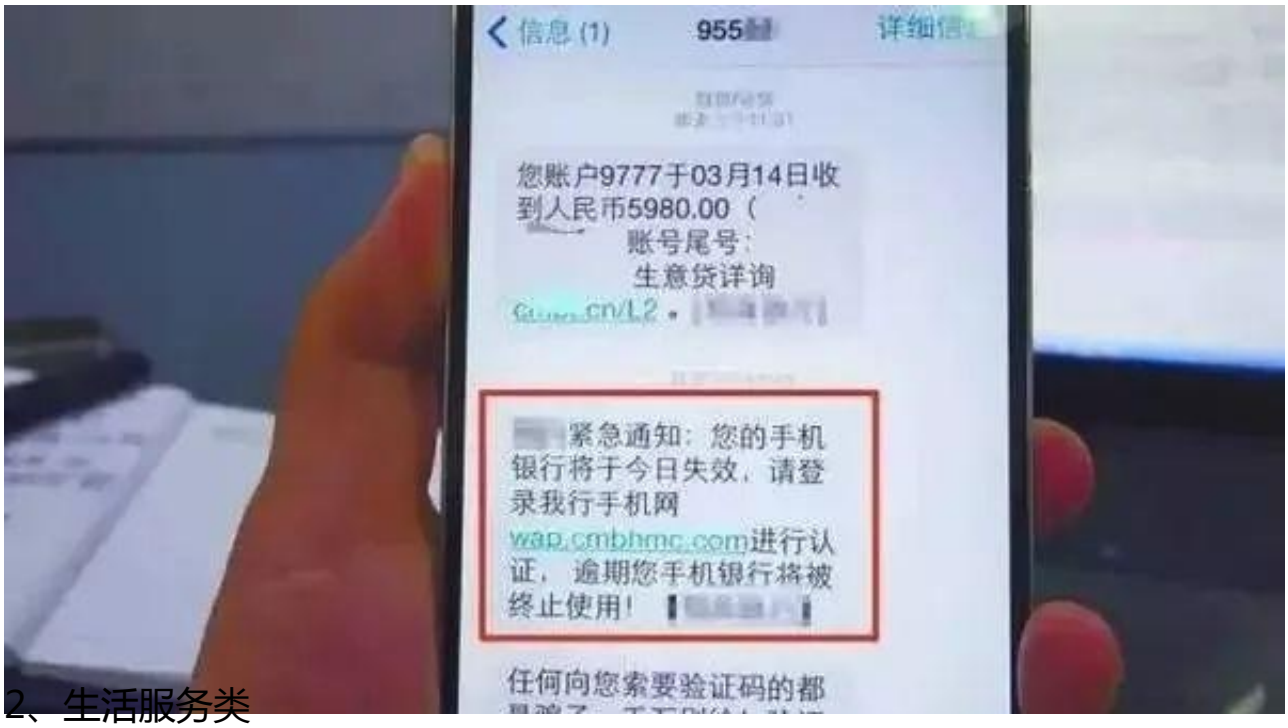
4、你竟然做出这样的事，实在让人不能原谅！

5、有人悄悄关注了你，点击了解！

如果点击这些信息中的链接就中了恶意木马程序。可能会窃取你手机上的网银、QQ、微信、支付宝等软件支付密码，盗取用户财产。各种诈骗套路五花八门、层出不穷。

03

还有哪些信息也不能相信？



2、生活服务类

如银行卡积分兑换，航班改签了。骗子通过这些信息，以诱骗你点开链接，仍然向视图扣除你银行卡里的钱。这些链接往往带有木马程序，跟很多钓鱼网站相链接。一旦点开之后，银行卡里的钱就危险了。

官方短信截图

3、充值诈骗

充100送200，充200送500。看这就很心动想点进去充值！且慢！如果你足够细心，应该可以发现，虽然该短信由“10086”发出，但其结尾处的
[中国移动]，与官方短信结尾处的【中国移动】，还是有所明显不同的。

提醒：短信冒充10086，迷惑性强。所有要填写银行密码，银行短信验证码的都是诈骗！

对于促销信息，请不要点击手机信息内所谓的充值链接，如确需充值，请至营业厅或者登录运营商官方的网上营业厅办理。

4、ETC诈骗短信

不少办了ETC的车主，接到号称高速ETC的短信。短信上称：“车主ETC审核流程未完成，需点击相关网页链接完成审核”。警惕！警惕！警惕！这个是假的，点开你就上当了！已有多地公安机关进行了辟谣，此短信为诈骗短信，如果收到，赶紧删除，千万不要点开链接！骗子的手法还是很多的，这里就不再一 一的举个例子了。

最危险的是短信内的不明链接，一不小心随手点击了，可真就上了骗子的当了。微信和支付宝，给我们带来便利的同时也存在不少安全隐患！以下这些保护账号安全的干货可以收下。

04

如何保护手机账号的安全？

第一招：开启应用锁

很多手机的安全中心或者设置中都有给应用加密的功能，给微信、支付宝、网银APP加上应用锁之后，每次打开它们都要解锁。虽然一些人也能破解应用锁，但是可以为你的手机卡挂失争取一点时间，毕竟手机丢失后，无论是电话求助客服，还是报警，走的流程较多，时间宝贵。

第二招：故意输错密码

手机被偷之后，马上借朋友的手机登陆自己的账户并故意多次输入错误密码，直到账户被冻结，支付宝被冻结后需要3个小时后才能再次尝试，但是通过找回密码，可以马上解冻，所以这个方法作用不大。之所以列出来，是因为有些小伙伴可能觉得这个方法不错，其实意义不大，在此提醒一下。

第三招：定期修改密码

微信、支付宝、聊天软件等重要账号单独设置密码，并定期更换修改密码，可有效避免自身账号被盗。

第四招：网聊不泄密重要信息

网络世界复杂，网聊需谨慎。切不可在网聊的过程中泄露自己的重要信息，包括银行卡号、手机密码、家庭住址、感情生活等信息。以防“有心”之人将这些信息作为盗窃你财物的“钥匙”。