看题目大家或许会想安全用卡与“码”何干？下面就由小编来告诉您。
随着手机支付功能的普及，打车、购物、缴费、转账等事务都可以通过手机分分钟完成，方便又快捷。但与此同时，手机支付类病毒、“有毒”的二维码等，也对支付安全造成了严重威胁。骗子们有哪些“新花招”？持卡人该如何应对？

手机支付病毒无孔不入安装软件要小心

最近，持卡人李先生遇到了一件糟心事，深夜睡梦中突然收到消费876元的“验证码”短信，让他意识到信用卡可能被盗刷，连忙打电话挂失，但正在这挂失的短短1分钟内，876元就被转走。挂失之后，他又收到几笔扣钱的“验证码”短信，好在因挂失及时都没有被转走。

据交通银行信用卡的安全技术专家介绍，这是典型的手机病毒侵害。由于李先生使用的是安卓手机，下载的客户端软件被内置了病毒，攻击者不需要拥有用户的手机，仅需通过网购钓鱼等手段获取用户的银行卡、身份证号等信息后，再利用手机病毒截取用户的验证码短信，就可以重置网购支付密码，盗取账户资金。目前，一种名叫“伪银助手”的病毒已经被二次打包到多个手机网银和支付应用中，散布在各大手机论坛、电子市场，由用户下载安装。该专家建议，用户在下载网银支付类应用时，最好到官方网站进行下载，同时，要及时为手机系统打上安全补丁，以阻止木马入侵；或安装安全软件，在木马装进手机之前将其查杀。专家强调，手机支付虽然方便又快捷，但没有绝对的安全，使用者应提高对手机支付安全性、风险性及操作性的认识，若发现问题，应第一时间与提供平台服务的商家或银行沟通，采取封锁账户或挂失等相关补救措施。

陌生“二维码”有风险别见码就扫

“二维码”也已经成为近期病毒入侵用户手机的主要模式。

赵小姐是一个网购族，经常用手机上网购物，可是资深买家也有马失前蹄的时候。她看到一家网店承诺购物能返100元购物券，觉得十分划算，就在店铺挑选了一件399元的连衣裙，并询问卖家如何获得购物券。卖家告诉赵小姐，只要扫一扫二维码就行，然后卖家把二维码直接发到了赵小姐的手机上。赵小姐扫后发现，并没有所谓的购物券，手机页面只显示出一个“淘”字。赵小姐明白自己上当了，于是急忙联系卖家，可卖家已经下线了。之后，赵小姐便收到莫名的消费短信提醒，遭遇了盗刷。

交行信用卡的安全专家给出了这样的解释：赵小姐扫的二维码是一个木马病毒。二

维码是网络链接的另外一种形式，打开了这个网址就是打开了一个木马病毒的下载地址。这种病毒被下载后，可自行安装，潜伏在手机后台中运行，并且不会在桌面上显示任何图标，赵小姐的信息就这样被悄无声息地盗取了。所以，手机用户在使用扫码支付时，应该保持谨慎，不要盲目扫描来历不明的二维码，要看清发布二维码的平台、付费场景和环境，尤其不要轻易相信他人发来的二维码。同时，手机用户应保护好自己的信息，即使用手机和银行卡或信用卡绑定，也不要在这张卡内储存过多资金，避免损失过大。

信用额度翻了倍实为骗子障眼法

小张交了女朋友，收入又不高，总觉得信用卡额度不够用。前不久，一个QQ群里突然有人打出广告，“代办提高信用卡额度”，小张立即和对方联系。对方告诉小张，他们可以通过银行内部关系帮他提高额度，同时，对方还发来了申请提高信用额度的“申请表”，要求小张填上信用卡及个人身份等信息。3天后，对方联系小张，让他查询信用卡额度。小张一查，额度果然翻了一番。可好景不长，就在第4天，当小张拿信用卡消费时，却被告知卡已经被刷爆了。这时，小张意识到自己被骗了，那个帮忙提额的人再也没有上线。

警方调查后发现，“小张的信用卡消费额度貌似提高了，但仅仅是一个临时额度，有效期仅有1个月”。交行信用卡安全专家表示，犯罪分子就是利用了持卡人急于调额的心理，骗取用户信息，再冒充用户，打进客服咨询调额。所以，客户泄露个人信息，委托他人办理业务，等于是把自己的信用卡亲手交给别人去盗刷，风险很大。一般情况下，交行信用卡会根据持卡人的历史用卡情况调整信用额度。持卡人若有临时用卡需求，也可以直接拨打卡片背面客户服务热线，申请临时调额。银行往往不接受任何第三方代理的调额申请。如果有疑问，持卡人应向银行官方客服咨询，切莫将自己的银行卡、身份证等重要信息随意告知他人。