春节临近，六类微信红包千万别碰！

春节临近，小伙伴们又开始摩拳擦掌，准备在抢微信红包的“事业”上大干一番。但与此同时，各种红包骗局也多了起来。

抢红包外挂助手暗藏杀机

杀机1：植入恶意代码泄露信息

调查发现，不少抢红包外挂软件会植入恶意代码，试图获取用户的地理位置、银行卡账号、手机联系人等机密信息。一旦用户允许软件获取这些权限，个人信息就很容易被不法分子上传到外部的C&C服务器(远程命令和控制服务器)之中。

杀机2：恶意广告、偷耗流量

此外，不法分子还会在其中嵌入广告与应用的推送代码(事实上，这也是大多数抢红包外挂的盈利手段)，在通知栏、桌面、移动应用窗口中弹出恶意广告，甚至还会在后台默默下载推广应用，耗费用户的流量，造成用户手机费用高涨。

杀机3：灰色软件，有安全隐患

目前，抢红包外挂软件属于微信明令禁止的软件，是难以获得安全认证的灰色软件，因此用户很难找到下载此类软件的安全通道。获得最高系统权限的安卓手机和“越狱”后的苹果手机会因为此类软件的下载而产生安全隐患。另外，抢红包软件的原理和代码已经在网络上广为流传，不法分子很容易在其中植入恶意代码，将其封装成为全新的软件供用户下载。

以下六类红包千万别碰

1、需要个人信息的红包不要碰

领取红包时要求输入收款人的信息，比如姓名、手机号、银行卡号，这种很可能是诈骗。而事实上，正规的微信红包一般点击就能领取，自动存入微信钱包中，不需要繁琐地填写个人信息。

2、分享链接抢红包是欺诈

有些朋友圈分享的红包，比如送话费、送礼品、送优惠券等，点开链接要求先加关注，还得分享给朋友。这种红包涉嫌诱导分享和欺诈用户，点击右上角举报即可。

3、与好友共抢的红包需谨慎

朋友圈有不少跟好友一起抢红包的活动，要求达到一定金额，比如100块才能提现，玩这种游戏要格外注意，红包页面的开发者是否正规，很可能只是一种吸引粉丝的骗局。

4、高额红包不可信

单个微信红包的限额是200元，因此如果收到比如“666”、“888”之类的大红包，基本上可以确定就是假的。

5、警惕“AA红包”骗局

业内人士称，此类红包往往对微信AA收款界面进行略微改动，加上“送钱”、“现金礼包”等字样，让用户误以为是在领红包。

6、拆红包输密码恐有诈

如果有商家或者朋友发来一个微信红包，拆开时却要输密码，那就要警惕了。

因为这很可能是假红包，真正的微信红包在收的时候是绝对不需要输入密码的。还要注意的是，有不法分子效仿“双11”时一些电商发红包的做法，发布山寨网页，借此收集网友的个人信息；或是通过点击量来增加公众号的阅读量，大家最好不要登录不熟悉或者是不正规的网站。

■来源：微信公众号“第一关注”

链接

支付宝、微信掐架春晚红包还能安心看春晚吗？

“双12”支付宝和微信的互掐还历历在目，这几天，为了春晚红包这事，这两家又掰起了手腕。事情的起因是这样的：支付宝拿下了今年春晚的独家合作，然后公布了“咻红包、传福气”春晚红包方案。微信也毫不示弱，9位数的投入金额也让人充满期待。

节日未到，有关红包的战争已经打响。估计春晚是不能好好看了，拼手气抢红包才叫过节。

支付宝：声波支付春晚亮相

支付宝为红包的预热已经开始了。不仅是支付宝界面有变化，其“咻红包，传福气”的广告语更是让人浮想联翩。目前在付款界面的下方，有一项声波付选项，点进去会传出“咻咻咻”的声音。支付宝方面已宣布，将通过该功能支持春晚红包活动。

除夕当晚，央视春晚直播的同时，观众根据春晚节目主持人的提示，打开支付宝就可以参与春晚互动。“咻”到红包的用户，可通过分享与亲朋好友一起拿红包，并有机会共同完成任务而获得更大的红包。目前已有华为荣耀手机、民生保险、瑞东集团、滴滴出行将借助支付宝平台，在春晚当天向全国人民发红包。

微信：朋友圈10天广告收入用来发红包

去年的羊年春晚，微信红包大放异彩，除夕当晚的微信红包收发总量达10.1亿次。尽管今年微信在春晚的较量中竞标失利，不过为了应对咄咄逼人的支付宝，微信宣布将除夕前后朋友圈10天的广告收入投入到“红包大战”中，价值5亿元的大红包将以现金形式发放！目前，微信公布春节红包的合作品牌包括太平洋产险、长安福特、恒大冰泉、东鹏特饮等。

■据搜狐公众平台