

治理信息骚扰仍需加把劲

日前,一位用户在网上曝光“短信退订难”,按照短信提示退订后,营销短信照发不误,用户找平台、找商家、找运营商,都没法彻底退订,引发不少议论。

无独有偶,最近一款名叫“寄生推”的恶意软件感染了300多款正规手机应用,通过云端控制给安装这些应用的手机推送弹窗广告,既让用户头疼,又损害了正规应用的声誉,再次引发了关于信息骚扰的话题。

《2017年中国手机安全状况报告》显示,近5年来,垃圾短信数量尽管有所下降,但总量仍然惊人。目前,中国移动电话用户超过14亿,平均每天花费近3小时看手机。用户基数大、使用频率高,垃圾短信、骚扰电话以及手机弹窗广告问题影响突出,治理信息骚扰仍需再加把劲。



“偷偷往你账户塞了30元红包,今天中午吃点好的。回T退订。”

“七周年特惠,品牌上新,半价秒杀,最后四小时,点击开抢!退订回复T。”

“恭喜您获得50000元现金贷额度,无需上门,最快2小时放款。回复TD可以退订。”

移动互联网飞速发展的今天,垃圾短信成了手机里的“常客”。在数以亿计的垃圾信息中,广告推销类短信占比高达98.1%。

尽管大多数营销短信末尾

■退订功能成摆设 ■用户丧失主动权

1、短信堆积如山

都有“回复T/TD短信退订”字样,但想退订可没那么容易。有的玩起语言游戏,比如“回复TD即可退订”,“复TD即可”才是真正的退订指令;有的对反馈置之不理,辩称“退订只针对本次活动,下次活动还会提醒”;有的甚至因为收到回复而认定用户活跃,反而加

大发送短信的频率。

2015年5月,工信部发布《通信短信息服务管理规定》,明确提出未经用户同意或请求,不得向其发送商业性短信息;用户同意后又明确表示拒绝接收的,应当停止发送。但是,通过短信平台代发短信的价格可以低至5分钱以下,还能点

对点把信息送到用户眼前,价格低、效率高、效果好,退订功能因此成了摆设。

记者登录淘宝网账户,进入个人设置页面,在消息订阅设置最下方找到营销提醒设置,发现系统默认卖家发布促销信息时将以邮件、短信等方式通知用户。记者关闭促销信

息短信提醒后,仍会偶尔收到来自淘宝网卖家的营销信息。去年“双11”购物节期间,仅11月10日一天,某款手机安全应用就拦截了1.44亿条营销信息。

中国人民大学商法研究所所长刘俊海认为,垃圾短信是公共治理的热点和难点。各部门要形成监管合力,打造信息共享、快捷高效的执法监管机制。此外,要鼓励广大用户积极举报,目前最便捷的举报渠道是向12321网络不良与垃圾信息举报受理中心反映。

今年3月,广东某公司经理张先生手机接到一个陌生男子电话,称如果不发200元红包,就要“呼死”张先生的手机和公司业务电话。张先生没有理会,结果在两个半小时内被呼了8000次。4月,犯罪嫌疑人莫某被抓获。此前他已在全国范围内敲诈勒索一个多月,非法获利万余元。

据了解,“呼死你”电话是指利用费用低廉的网络电话作为呼叫平台,在一段时间内对特定电话号码高密度集中呼叫,导致被叫电话无法正常使用的恶意呼叫行为。有的人因为网购商品不满意给出差评,有的人因为朋

友欠了网贷平台的款,甚至只是在路边填了个问卷,扫了个二维码,就遭遇持续不断的“呼死你”骚扰,不仅干扰了正常的工作学习生活,还因此错过重要电话,造成损失。

刘俊海说:“‘呼死你’这样的电话骚扰软件,侵害了公众的安宁权、休息权等人身权利。用户遭遇到这样的骚扰电话,要善

于固定和保全证据,及时截屏录音,向法院提起民事诉讼,同时也要向公安机关、工信部门投诉举报,追究不法分子的行政违法责任与刑事责任。”

业内人士指出,“呼死你”软件拨出的号码均为虚拟号,网站服务器多在境外,追溯和追责难度较大。由于号码数量庞大,手机一般只能逐个标记

拉黑或设置通信白名单,用户拦截难度也很大。去年9月,中国移动尝试推出“呼死你防护业务”,在此业务有效期内,陌生号码要按语音提示正确输入验证码后才能接通,靠软件机械拨打的“呼死你”因无法完成这个步骤而被拦截。

还有一些不法分子利用互联网改号软件,“李鬼变李逵”,

让被呼叫用户的手机上显示银行、公检法等权威机构的官方号码。今年4月,深圳警方破获一起新型电信网络诈骗案,犯罪嫌疑人非法获取大量信用卡用户信息后,利用改号软件冒充银行客服,以申请信用卡为理由开展诈骗,10余天内骗取700多万元。

“屡禁不止的骚扰电话,不仅让用户不堪其扰,更大的危害是可能隐藏其中的电信诈骗等违法犯罪行为。一方面要打击非法的‘呼死你’、改号软件,另一方面要打击公民个人信息买卖。”中国电子商务协会政策法律委员会副主任阿拉木斯说。

■骚扰来电难屏蔽 ■伪装号码难识别

2、电话轰炸不断

智能手机时代,为了争夺有限的手机内存资源与用户注意力,各款手机应用频繁推送各类信息,即时通信、新闻资讯、营销信息、更新提醒、早晚问候如千军万马过独木桥,动辄堵死信息通道,造成手机卡顿、死机的后果。有些手机应用还有意设置障碍,阻止用户关闭推送消息提醒。无计可施的用户只能要么忍耐,要么卸载了之。

前段时间,一款名叫《旅行青蛙》的手机游戏走红,为了拥有更多游戏货币“三叶草”,一位用户花费4.99元购买了“无限三叶草”套餐。按照商家要求操作后,用户发现购买的其实是一

款经常弹出广告的山寨应用,每条广告至少得看十秒才能关闭。

《互联网广告管理暂行办法》要求,互联网页面的弹出广告应能“一键关闭”,但手机屏幕上的弹窗广告如何管理,还缺乏明确规定。

烦人又黏人的极端弹窗广告当属恶意程序。最近,一款名叫“寄生推”的恶意软件感染了

300多款正规应用,通过云端强行给安装这些应用的手机推送弹窗广告。另一款名为“堕落系统”的类似恶意软件在今年3月的10天内,向受感染的手机用户强行推送1300余万次广告,诱导获得54万次点击,收入约70万元。

腾讯手机管家安全专家杨启波介绍,借助腾讯AI反病毒

引擎分析后,这类恶意软件已被查杀,但这一事件暴露出恶意软件越来越隐蔽。通过在“宿主”应用上留下“后门”,可以绕过大多应用市场和杀毒软件监测,用户一旦完成安装,“寄生推”就通过云端推送广告,防不胜防。

今年4月,中国信息通信研究院泰尔终端实验室倡导成立

的“安卓统一推送联盟”公布首批名单,加入联盟的应用将遵守《绿色应用公约》,限制过度推送信息、占用手机后台资源等行为。

复旦大学软件学院副院长韩伟力说:“随着第三方开发库的普及,当前手机系统安全生态和早期已有很大不同,建议规范手机应用开发,建立移动应用的准入制度,为用户提供能验证应用合法性、安全性的权威平台。同时要惩处‘寄生推’类恶意软件的运营商,追查通过恶意渠道推送广告的企业,从经济源头上斩断这些恶意软件的利益链条。”

资料来源:新华网

■频繁推送易死机 ■恶意程序更隐蔽

3、弹窗广告泛滥