

# 工信部将清理垃圾短信和伪基站

## 相关法规拟出台



6月13日,飞象网获悉,为斩断垃圾短信利益链条,工信部拟制定出台垃圾短信相关管理规定,为垃圾短信治理提供执法依据。同时将集中整治“伪基站”活动,对其产业链各环节进行集中整治。

近年来,垃圾短信严重侵扰用户隐私,据

消息透露,自2014年5月5日起至11月30日,工信部将开展深入治理垃圾短信净屏2014专项行动,以斩断垃圾短信利益链条。

消息称,工信部拟制定出台《通信短信息服务管理规定》,为垃圾短信治理提供执法依据,制定出台并推动落实《短消息网间联动平台技术要求》等8项反垃圾短信技术标准。

与此同时,工信部还将配合公安等相关部门加大对利用垃圾短信实施诈骗和对“伪基站”破坏公用电信设施、扰乱电信市场秩序行为的惩罚,并联合工商等相关部门对垃圾短信广告主和“伪基站”产业链各个环节开展集中整治。

对于基础运营商,工信部表示鼓励其利用大数据、云计算等新兴技术,健全网络收、发端垃圾短信处理系统;跟踪研究 iMessage 垃圾信息、骚扰电话等新情况、新问题的技术监测和防范手段。并组织落实手机实名制,实

现对个人号码发送垃圾短信的溯源和治理。

2013年4月~12月,工信部启动了“深入治理垃圾短信息专项行动”,建立了垃圾短信网间联动处理机制,举报量下降80%;并组织起草了《通信短信息服务管理办法》,完善了垃圾短信治理规章制度。

另据了解,工信部还将启动对移动智能终端应用传播淫秽色情信息的整治,全面排查应用商店,清理下架违法违规APP。并加强移动智能终端预装管理,规范预置APP行为,加强移动智能终端进网安全检测和管理,加强技术手段建设、组织开展APP检测。

根据此前消息,中国移动也正在谋划成立全国在线服务公司,集中处理中移动用户在移动互联网上遇到的问题,加大力度治理垃圾短信、持续打击恶意软件和不知情定制行为、严查狠打手机淫秽色情网站、全力推进电信客户实名制。(据飞象网)

# 揭秘微信六大骗术:代购点赞上榜



微信的使用带来各种便利,但也会带来一些麻烦。合肥警方日前向社会发布提示,“朋友圈”有时也会坑你没商量,经常使用微信注意防盗防骗是一门必修课。

根据接到的报警和案件,合肥警方罗列了六大类微信诈骗手法:

一是利用代购诈骗。诈骗者声称能“海外代购”,待顾客付了代购款之后,诈骗分子会

以“商品被海关扣下,要加缴关税”等类似的理由要求加付“关税”,等顾客钱付了,货品也收不到。

二是利用二维码诈骗。诈骗者以商品为饵,给顾客返利或降价,再发送商品二维码,实则木马病毒。

三是盗号诈骗。此种诈骗与盗用QQ号诈骗类似,诈骗者冒充家人联系,并以各种理由要钱。

四是身份伪装诈骗。诈骗者一般装成高富帅或者白富美,搭讪,或骗取感情的信任,进而以借钱、商业资金紧张、手术等为由骗取钱财。

五是点赞诈骗。现在这种诈骗方法最多,常常要求参与者将自己的电话和姓名发到微信平台,一旦所征集的信息数量够多了,这种“皮包”网站就会自动消失,目的是套取更多人的真实个人信息。

六是微信假公众账号诈骗。诈骗者喜好在微信平台上取类似“交通违章查询”这样的公众账号名称,让人误以为这是官方账号,然后再进行诈骗。

(据中国网)

## 移动 4G

## 大举收复 3G 失地

以旧换新,实为收复失地

河南移动最近推出一项“以旧换新”的举措,行动比较低调,但直指竞争对手的3G有生力量,移动此举意欲收复在3G时代失去的领地。

用户(不分运营商,不分种族,不分男女老少),只需携带手机和机主本人身份证,即可在移动营业厅换取4G版iPhone5s。

可参与活动的手机为苹果和三星的高端机:iPhone4,iPhone4s,iPhone5,三星S3,S4,NOTE2,NOTE3。

举个更详细的例子吧,目前市场上的三星S4除移动版之外有三个版本:I9500(公开版,只支持联通3G)、I9502(联通3G版)、I959(电信3G版)。这三款,都可以去移动营业厅换iPhone5s。

换新过程是这样的:不需要发票和配件,只要是大陆行货,没有维修记录即可。由移动营业厅对旧手机进行评估,根据手机品牌、型号、新旧程度,评估出折旧费。三星NOTE3最高折价4289元,换一部4G版iPhone5s的话,用户只需再掏199元。

4G 歼灭战低调开战

三家运营商4月份的运营数据,想必诸位看官都有印象。移动是唯一一家从2月份就开始单独公布4G数据的,2月4G用户总数134万户,3月279.3万,4月479.8万。以倍增的速度发展。3月净增145.3万,4月净增200.5万。

站在用户口碑层面看,4G已带动移动全线回归,满血复活。从网络覆盖,到营销推广,移动终于又体会到了强势运营商的赶脚。3G时代移动要看手机厂家的脸色,4G时代手机厂家又开始追着移动转……

4G在数据上已经击退了各种3G,在认知领域已经成为时尚新名词,在用户选择上成为风向标、人心所向。于是,一场歼灭战,也是收复失地之战,悄然拉开。

眼看着就要将移动送上重返垄断、一家独大的舞台,中国愤青们的内心很是复杂。说它垄断,讨论是TDD还是FDD,可是,这跟我等小民又有何干?还是看看世界杯期间谁的速度够直播,谁提供的免费流量多,其他的交给该死的中国国情吧。(戴黎明)

# 无需密码手机能读银行卡

## 专家:被恶意使用可能性小



近日,有网友爆料称,无意中手机放在银行卡之上,手机竟然迅速“扫”出了银行卡最近的数字详细交易信息。NFC手机能轻松读取芯片银行卡卡号及交易记录,会威胁银行卡里的资金安全吗?

记者试验发现,如果用户的智能手机有NFC功能,只要开启该功能并靠近IC芯片银行卡,手机就可以在无需输入银行卡密码的情况下“扫”出卡内近期详细交易数据。不过,不同银行的卡片能读出的信息含量不一样,有些银行卡可以轻易读出卡片余额、最近10笔详细交易记录、持卡人姓名甚至身份证头尾两位数,有些则只能读取卡号最后四位数等简单信息。

对为什么金融IC卡的信息可以被NFC手机读取的问题,银联技术专家徐静雯分析认为,金融IC卡信息被读卡器明文读取符合国际规范,目的是为了便利持卡人交易使用。

金融IC卡通过非接方式读取部分信息,可以进行快速数据传输,才能进行非接快速的小额支付。

徐静雯指出,非法读取他人金融IC卡信息需要具备相应的条件。受手机电磁场复杂环境等因素影响,NFC手机与卡片的距离需要在2厘米以内才能有效读取。丢失金融IC卡片和丢失载有个人身份信息的证件在被非法获取个人信息上的性质基本相同。

同时,银联技术专家进一步指出,非法读取的信息被恶意使用的可能性较小。部分持卡人担心通过电话银行提供交易明细更改密码盗取账户内资金。事实上,按照银行业业务标准流程,被读取的信息难以有效回答电话银行所设的安全问题,无法通过电话银行进行交易欺诈,同时由于缺乏身份证复印件等信息,也无法办理信用卡进行欺诈,信息被恶意使用的可能性较低。同时,非法读取信息的金融IC卡片不可能被复制,持卡人资金安全能够得到较好的保障。金融IC卡以智能芯片为介质,具备全方位的安全体系,即使部分

卡片信息被读取,仅凭读取的相关信息也不可能复制出金融IC卡,持卡人资金安全能得到有效保障。

## >>>链接

## 什么是 NFC

NFC(近场通信),又称近距离无线通信,是一种短距离的高频无线通信技术,允许电子设备之间进行非接触式点对点数据传输交换数据。与目前使用较多的蓝牙技术相比,NFC使用更加方便,成本更低,能耗更低,建立连接的速度也更快,只需0.1秒钟。但是NFC的使用距离比蓝牙要短得多,有的只有10CM,传输速率也比蓝牙低许多。

(据《京华时报》)