编辑 吴辰光 美编 胡潇 责校 杨志强 电话:64101903 itsmzk@163.com

4G冰火效应愈加强烈

联通电信苦等FDD牌照

近日，三大电信运营商相继公布了2015年1月运营数据：中国移动4G用户突破1亿大关，而中国联通则创下新增用户历史新低，中国电信用户数增长同样缓慢。中国联通和中国电信热切盼望的FDD牌照并未如传言一样在农历春节前发放，在4G冰火效应愈加强烈的情况下，中国联通和中国电信还能等FDD牌照多久？

1月数据显示，中国移动4G用户数保持高速增长，自商用一年多来已迈过了1亿户大关，4G用户数达1.06797亿，而移动电话用户总数也达到8.0855亿。

与中国移动高增长形成鲜明对比的是，中国联通在1月仅新增移动电话用户8.3万，创下历史新低，移动用户累计达到2.9918亿户，其中3G/4G用户数1.49989亿户。

而中国电信在该月净增移动电话用户105万，其中3G用户净增212万，移动电话用户总数达1.8667亿，虽然相比去年前三季度有触底反弹迹象，但原本在三大运营商处于较弱地位的中国电信追赶中国移动仍显吃力。

值得注意的是，中国移动与中国联通、中国电信的冰火两重天局面已持续了一年之久，4G成为最直接的影响因素。中国移动利用TD-LTE牌照先行发放的优势得以抢跑，再加上其雄厚的资金、人力等资源实力，TD-LTE网络狂飙突进地覆盖国内，终端厂商积极调整产品线，加大4G机型的研发和上市步伐，这使得中国联通和中国电信失去了时间窗口，原本计划利用成熟度更胜一筹的FDD网络优势一步步被消减，中国联通和中国电信在3G时代好不容易从中国移动口中抢夺来的用户又一步步回流至中国移动的怀抱，这样中国移动一家独大地位更加明显。

鉴于此种情况，FDD网络全面放开已成为迫在眉睫的事情。尽管工信部去年已放开了TD-LTE/FDD混合组网的试验许可，这被业界视为为FDD网络全面开放铺路，中国联通和中国电信也得以在国内50多个城市内启动FDD网络，但在网络覆盖、业务创新、品牌营销中仍然未能放开拳脚。

尤其是中国电信，受制于CDMA网络的技术演进，4G终端机型匮乏，严重制约4G发展，更难提与其他运营商竞争。不过为此中国电信已铆足力气要在2015年斥资160亿元推动天翼4G终端发展，打造100款4G精品终端。

对此，业内观察人士指出，FDD牌照发放不应该再犹抱琵琶半遮面，在中国移动4G商用一年多以来，国内消费者已对4G形成刚性需求，4G换机需求日益增长，因此全面放开4G竞争已远远大过先行培育TD-LTE市场的战略需要。

另有一种悲观论调称，即使全面放开FDD牌照，中国联通和中国电信也很难改变中国移动一家独大格局，在此基础上业内还一度传出中国电信和中国联通合并、电信业重组的消息，不过监管部门对此予以否认。从中也可见中国联通和中国电信的捉急。

电信分析师认为，中国移动TD-LTE在国内市场上已抢先了FDD一年多的时间，随着TD-LTE网络在信号覆盖、网络稳定性、终端使用体验等各方面的提升，中国联通和中国电信能够等待的时间已很少了，FDD全面放开已迫在眉睫。就在此前不久，工信部部长苗圩公开表示，年内条件成熟将有望发放FDD牌照。

北京商报记者 吴辰光 曲忠芳

·茶座·

联想摊上事儿了

吴辰光

这个春节，身为PC老大的联想过得并不舒心，原因是日前联想被曝部分型号的笔记本电脑中预装Superfish软件，如果只是推送广告倒也不至于引起太大的风波，但据相关机构专家称，该预装软件存在安全漏洞，威胁用户信息数据安全。

Superfish是一款广告应用插件，此次涉及的是2014年9月至2015年1月期间售出的部分型号联想笔记本电脑，用户在首次激活电脑时会自动安装Superfish。问题的主要症结在于Superfish会为自己颁发一个可信赖证书，然后在系统中安装带有自己签名的CA认证。简单来说，只要借助有效密码及适当的软件，与存在漏洞的联想电脑用户处在同一个WiFi网络中的任何人都有可能监视该用户，或者向其数据流中植入恶意软件，造成严重的外部攻击。

不得不说，自2013年“棱镜门”曝光以来，全球各国政府、消费者都开始重视起网络信息安全，甚至谈漏洞风险色变，因此联想此次“插件门”即便看似小事儿一桩，却引起了强烈的反响，连美国国土安全部也发布了Superfish安全隐患的警示信息。

联想在向媒体发出的回应声明中称，在中国内地销售的消费类笔记本电脑并未预装过Superfish软件。不过，鉴于联想在国内市场及全球市场庞大的出货量，恐怕很难彻底打消消费者的疑虑。

好在联想目前也已意识到了事态的严重性，发布了自动卸载Superfish的工具，并从网络浏览器中移除认证。联想还表态正在与McFee、微软合作，使用其安全工具和技术自动隔离或删除Superfish软件及认证，并自动修复漏洞。

从“棱镜门”，到好莱坞女星iTunes照片泄露事件，再到联想“插件门”，我们看到，PC、智能手机等各类连网设备均有可能遭受到网络漏洞及安全风险，关于网络风险的披露与曝光消息会越来越多。在这种情况下，消费者的警惕性和安全意识也在相应地不断提升，网络安全也有望不久后成为消费者选购产品及品牌的一个重要影响因素，可以预见，终端厂商也会相应地对产品的安全把关，甚至在品牌宣传中，保障用户上网安全也有可能成为主打卖点之一。

骚扰电话2014年常见骗术大起底

据搜狗号码通日前发布的《2014骚扰电话年度报告》显示，2014年全国全年骚扰电话总数高达270亿通，其中公众接收到的“响一声”占比最高，达到42.7%；其次为涉嫌诈骗类（26.3%）、理财和推销类(18.6%)、房产中介类(12.3%)。

深入调研分析获知，2014年与2013年比，响一声及其他骚扰电话的占比变化不大，但是涉嫌诈骗的占比增长了很多，最近3个月期间，响一声发生率达到63.3%，而涉嫌诈骗类发生率最高的中奖电话，占比达到20.8%。随着春节到来，诈骗分子为了得到更多的“年终奖”和“压岁钱”开始大量作案，诈骗手段层出不穷、不断翻新，欺骗性和再生性极强。

除了中奖电话以外，公众感知危害较大的还有冒充熟人、公检法打电话进行恐吓，诱导用户回拨，此类诈骗电话是2014年最流行的一种诈骗手段，据了解，最新的骗术是“叫爸妈”，接到此类电话切忌回拨，要提高警惕多加小心。

对此，搜狗号码通提醒广大电信用户，涉嫌诈骗类电话大多有一个共同的特点，即表面上被害人会获得较大的利益或被胁迫，并最终会与“财”或“色”关联起来。新春之际，为了全面帮助用户识骗，搜狗号码通对常见骗术进行大起底。

类型一：中奖电话

近几年，不少诈骗分子冒充“热门综艺节目官方”身份，向被害人打电话散布中奖消息，并发送被害人中奖查询网站。而该网站系与实际官网样式风格非常相似的钓鱼网站，很容易以假乱真，让被害人误以为自己中奖，不法分子进而以缴纳个人所得税、手续费等为由，向被害人实施诈骗，相似的骗术还有“赠送物品”等。

报告特别提醒，不法分子以各种娱乐栏目等方式诈骗的案件屡有发生，群众在观看娱乐节目后，要提高防范意识，谨防上当受骗，不要贪便宜，要保持理性。而手机用户可以使用搜狗号码通等手机防骚扰工具进行拦截或拒接，切勿接收来历不明还要付款的包裹。

类型二：冻结账户

互联网金融的发展又给不法分子带来新的契机，他们通过使用拨号器撒网式拨打电话，以播放录音的方式称受害人的支付宝、网银、社保卡、医保卡账户发生异常，需要冻结，并提示事主拨打所谓的公安局或检察院电话以协助调查。所谓的公检法部门工作人员则要求事主将银行存款转至“安全账户”进行保护。

此类诈骗方式常见于经常网购且对安全信息不了解的电信用户。对此，搜狗号码通提醒广大网购爱好者，在电商为大家带来全新购物享受的同时，对个人信息安全，尤其是个人金融安全，还需提高自身的防护能力。商家制定了严密的规则，具有极高的保护作用。

类型三：冒充熟人进行诈骗

前段时间，很多网友都反映说接到了来自“领导”的电话，或者是与“熟人”玩起了电话版“猜猜我是谁”，几番寒暄后话题就转到“钱”上，借口推销书籍、纪念币、划拨款项、配车、帮助解决经费困难等，让受骗单位支付订购款、手续费等到指定银行账号实施诈骗。

对此，不要盲目听从“领导”或“熟人”电话、上级指示，要保持清醒头脑，通过正确渠道核实人物身份、电话号码以及事情真伪。

类型四：冒充公检法进行恐吓

据用户线上调研结果，借公安、法院名义传达通知涉嫌诈骗的手段的危害仅次于中奖类。不法分子利用受害人畏惧公检法部门的心虚与软弱心理，对受害人施压，击溃其心理防线，从而获取到被害人银行账户和密码等信息，常见于“快递有问题”、“电话欠费”、“涉嫌贩毒、洗黑钱案件”、“汇钱救急”、“遭到绑架”等场景。

此外，还有“快递未取”、“低息贷款”、“400开头的来电”等几种骗术也很常见，在此提醒广大市民增强风险防范意识，遇到此类电话或短信，不要轻易泄露个人信息或向陌生人转账付款，并可以通过各快递公司的官方咨询确认，以免上当受骗，损失财物。

以上种种电话诈骗案例不胜枚举，骗术花样层出不穷、防不胜防，用户需要注意的最关键一点是，不管对方冒充的是老板、警察、法官还是亲戚朋友，无论他怎么忽悠，最后一旦提到汇钱，那就是诈骗，捂紧钱袋，不要汇款，同时下载安装搜狗号码通到手机，最大程度防骗。

北京商报记者 吴辰光