工信部:

先期投入3亿元 开展5G技术研发

记者昨日从工业和信息化部获悉,我国已经在5G关键技术等方面取得了积极的进展。业内人士认为,随着5G技术的快速推进,设备厂商有望最先受益。

工信部人士介绍说,2013年2月,工信部与科技部、发改委联合支持成立了IMT-2020(5G)推进组,以此为平台,集中产业研用优势单位联合开展研发和国际标准推进工作。IMT-2020(5G)推进组已经在需求愿景、关键技术等方面取得了积极的进展。

同时,主管部门还投入了约3亿元,先期启动了国家863计划第五代移动通信系统重大研发项目。目前,5G的第一阶段和第二阶段目标均已达成,包括密集网络部署、多天线阵列技术、用户速率、发射功率、频谱效率、能耗效率等与4G相比具有大幅度提升。

目前研究显示,5G速率为4G的10倍至100倍,可达10GB/S,并将因此带来更多的杀手级应用。

专家认为,在这个过程中,设备生产的龙头有望成为产业链率先受益的群体之一,因为运营商和设备商都认识到,到了5G时代,需要利用过往2G/3G/4G网络部署所基于的标准技术,而不是完全抛开历史,去发明一种全新的5G技术。这意味着现有设备龙头的竞争优势将更加明显。目前,中兴通讯和华为都已经投入重金致力于5G的研发。

(据《中国证券报》)

通信工作室
负责人:戴黎明
电话:13803769176
E-mail:xyrbsm@163.com

“微信电话本”被木马篡改

恶意扣费泄隐私

“免费通话”的微信电话本近日火了起来,引发了市场的广泛关注,以至于一度下载量过大,造成后台运行故障。

360手机安全中心发布安全播报称,首次监测到“微信电话本”应用被木马篡改,能遍历中招手机的通讯录向所有联系人群发短信,还能在后台私自发送扣费信息,甚至判断手机中是否安装了安全软件来躲避查杀。

安全播报指出,假冒的微信电话本会使用三招掩人耳目,潜伏在手机中作恶:

假冒图标。采用与正版微信电话本极其相似的图标和界面,能正常登录及收取短信验证码,具有极强的欺骗性。

躲避查杀。该木马会判断中招手机中是否安装了安全软件,如果没有安装,其还具备遍历中招手机的通讯录,并向所有联系人群发短信的能力,可能给手机用户带来话费损失。由于正版微信电话本同样会读取手机通讯录信息,手机用户很难通过安装应用时的隐私权限识别安装的软件是否为恶意程序。

屏蔽短信。木马会通过中招手机私自发送恶意扣费短信,并屏蔽运营商的回馈短信,这样,手机用户就在不知不觉中被订制了扣费业务。

专家建议,手机用户使用微信电话本一定要通过官网或安全可靠的手机应用市场下载,避免从朋友圈分享、论坛、云盘等渠道下载到被恶意篡改的假微信电话本应用,造成话费损失和隐私泄露。

(据新华网)

伪基站死灰复燃

手机用户要提高警惕谨防被骗

靠一根天线、一台电脑和发射器向群众发送垃圾、诈骗短信的伪基站如今又在多地死灰复燃。仅在宁夏,近5天内就查获3起利用伪基站恶意发送短信事件,通信运营商提醒手机用户,请勿轻信任何非正常渠道所提供的促销活动信息、中奖信息,不要轻易点击来源不明的网址、验证码等,以免上当受骗。

记者从中国移动宁夏公司和宁夏无线电管理委员会办公室获悉,连日来,宁夏区内5个地级市均多次出现利用伪基站发送诈骗信息的情况,一些伪基站甚至假冒中国移动10086客服号码发送诈骗信息。

据了解,伪基站也称小区短信发射系统、圈地短信发送平台等,是一种实施电信诈骗的高科技仪器,这种设备能在人群密集的场所移动或固定发射,且能搜集以其为中心、一定半径范围内的手机信息,之后强行发送诈骗信息或垃圾短信。

通信运营商表示,他们将会同无线电管理部门和公安部门加大对伪基站打击力度,维护网络信息安全,同时提醒广大手机用户收到“银行卡密码升级”“中奖”或要求转账之类的短信,尤其是与附近手机用户同时收到内容相同的短信时,要提高警惕,不要轻易点击短信中的链接,更不要转账、汇款。 **(据新华网)**

“双十一”网购诈骗上当七成是男性

亲,“双十一”抢的iPhone6二手便宜卖给你要吗?千万小心,也许这只是骗子的鱼饵——13日,针对“双十一”期间的网络安全状况,360互联网安全中心发布《2014年双十一中国网购安全专题报告》,报告显示,“双十一”购物狂欢季落幕,江苏成钓鱼网站重灾区;90后网购者被骗的最多;相比女网友,男网友更容易受骗。

江苏遭密集钓鱼攻击,全国拦截1.97亿次

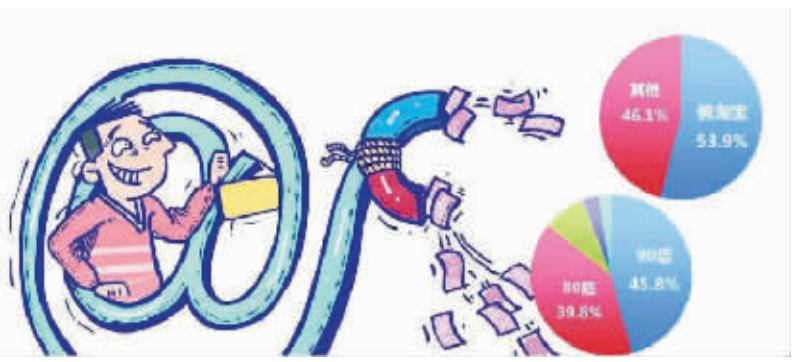
记者在中国网购钓鱼地图上看到,“双十一”当天全国共拦截钓鱼网站攻击1.97亿次,相当于平时日均拦截量的2.05倍。而江苏、浙江、福建、广东等沿海经济发达地区也是钓鱼网站攻击密集的地区,显示攻击的红点几乎密密麻麻列满了地图,而相对来说中西部地区遭受的攻击较少。“双十一”当天,广东用户遭到钓鱼网站攻击的次数最多,高达2896万次,而广东同时也是当天网购交易额最高的地区。

另据监测,“双十一”期间共截获新增假冒淘宝的钓鱼网站3288个,占全天新增钓鱼网站总数的53.9%。

360专家告诉记者,从钓鱼网站内容的分析来看,出现的假冒淘宝网站主要集中为两种类型,一类是以“淘宝异常订单处理中心”为代表的专门用于退款欺诈的钓鱼网站,另一类是以假冒二手淘宝为代表的虚假二手交易平台。

江苏网购被骗者南京苏州最多,男网民更好骗

“双十一”期间,目前从报案受骗者归属地上看,广东、江苏、河北是“双十一”当天国内网购被骗报案人数最多的地区,江苏又以南京和苏州两地遭遇的钓鱼攻击最多。



根据受害用户报案情况看,受骗者主要集中在20岁至29岁之间,占所有受骗者总人数的58.6%。其次是30岁至39岁的受骗者,而在所有报案的受骗者中,年龄最小的为12岁,年龄最大的为59岁。

从中可以看出,无论怎样划分年龄段,能熟练使用电脑,喜欢上网购物,但又缺乏足够社会经验的年轻人都是网络诈骗的主要目标和主要受害群体。

另外,在所有报案的受害者中,男性占比高达72.8%,女性比例为27.2%,受骗男女比例接近2.7:1;男性网民在“双十一”的人均被骗损失为1922元,而女性网民的人均被骗损失为1183元。这表明尽管“双十一”期间有大量女性参与抢购,但女性网民在此期间更倾向于选择自己习惯的或者相对安全的消费环境。

专家提醒:“双十一”后警惕3类网络诈骗

360互联网安全中心专家根据最近一年流行的网络诈骗形式,提醒广大网民警惕“双十一”后可能大规模爆发的三类高危网络诈骗。

1.退款诈骗:以网购交易存在异常或无法发货为由,通过退款诈骗钓鱼网站进行诈骗是今年最为流行的网络诈骗方式。专家提醒:“卡单”“掉单”“交易异常”“解冻订单”“异常订单处理”等词汇全是诈骗术语,正规电商交易平台上不会出现这些词汇。

2.二手交易诈骗:“双十一”之后的一星期,二手交易诈骗会大幅增加,且多以手机和家电为主。刚刚上市的iPhone6,很可能会成为“双十一”后二手交易诈骗的重灾区。

3.中奖诈骗:网民接到此类信息如有疑问,需拨打电商网站的官方客服电话确认,切忌直接拨打短信中的联系电话,也不要轻易点开短信中任何网址链接。

(据《扬子晚报》)

360报告称

今年三季度垃圾短信大幅下降

360互联网安全中心最新发布的《2014年第三期中国手机安全状况》显示,不论是从垃圾短信的拦截量还是举报量来看,2014年三季度的数据较二季度都有大幅下降,分别环比下降41.5%与20.1%。

报告分析认为,垃圾短信的大幅减少主要与两方面的因素有关:一是工信部对垃圾短信展开的持续近一年专项治理取得了成效;二是手机安全厂商通过智能语义拦截算法的不断改进,也逐步使得垃圾短信的生存空间越来越小。

据介绍,2014年二季度,360手机卫士共拦截各类垃圾短信176.8亿条,平均每天拦截垃圾短信1.94亿条。用户举报各类垃圾短信5824万条,平均每天举报垃圾短信64万条。

2014年三季度,360手机卫士共拦截各类垃圾短信103.4亿条,平均每天拦截垃圾短信1.12亿条。用户举报各类垃圾短信4652万条,平均每天举报垃圾短信50.6万条。

从三季度用户举报的垃圾短信的内容来看,广告推销类垃圾短信数量依旧最多,占比高达72.8%;其次为诈骗信息、违法信息的垃圾短信,占比分别为14.5%和7.6%。**(据新华网)**