**小心：你的手机可能正在泄密**

    日前，一则关于手机是如何泄密的新闻被各大新闻网站转载。手机已经成为人们生活的必备品，通过手机接入互联网的用户占网民总数的近80%，已超过电脑成为我国网民的第一大上网终端。手机一旦遭受恶意软件、病毒的侵袭，极易泄露个人隐私，损害手机用户经济利益。手机如何防偷窥、防泄密的问题，越来越受到人们重视。

**92.5%的用户习惯将隐私放在手机中**

    根据360手机安全中心此前联合DCCI发布的一份《中国Android手机用户隐私安全认知调查报告》显示，有92.5%的用户会将隐私存放在智能手机中，让手机成为了存放用户隐私最多的设备，也让手机彻底变成了“手雷”。



    截至2015年4月，我国共有手机用户12.93亿，不少人还拥有两部以上手机，每年全国淘汰和废弃的手机约1亿部。与此同时，近年来我国手机遭到恶意软件攻击的数量也不断攀升，隐私泄露已经司空见惯。被窃取的信息主要包括个人位置信息、通信信息、账号密码信息、存储文件信息等四大类。

**手机泄露个人隐私的四大途径**

    调查显示，安卓手机应用程序不完善、审核不严、旧手机隐私泄露、手机木马窃取隐私成为安卓手机隐私泄露的主要途径。360发布的《中国Android手机用户隐私安全认知调查报告》也显示，因为安卓APP应用程序本身不完善，各类安卓应用存在严重的隐私获取“越界”现象，更使得手机成为隐私泄漏的一大渠道。



    有关研究显示，Android系统已经成为恶意软件的重点感染对象，国内市场中近六成的Android应用程序有问题，约有四分之一的安卓用户隐私遭到泄露威胁。Android手机软件对位置、通话记录等核心隐私权限越界严重。11.2%的手机软件越界读取位置信息，9.4%的手机软件越界读取通话记录。

    专家指出，其主要原因就在于Android是开源的，软件用户有自由使用和接触源代码的权利，可自行对软件进行修改、复制及再分发。有些用户还会自己对系统进行破解，获取权限。这些都是造成Android平台泄露个人信息的重要原因。



    目前，窃取隐私的手机木马主要通过三种方式传播，一是将木马隐藏在彩信中，以诱人标题骗取用户点击或运行。或将恶意代码隐藏在“空白短信”中，一旦用户打开短信，手机系统后台就会自动下载恶意软件。二是伪装成手机常用应用软件，如游戏、安全补丁、免费资料以及电子书等，上传到部分缺乏安全验证的中小手机软件论坛中骗取用户下载安装。三是将窃取隐私类手机木马预装在手机ROM中，通过刷机包或水货手机扩散传播。

**如何防止手机成为隐私泄露源头？**

    首先，要养成良好的手机使用习惯。不要轻易接听、接收陌生人的电话、短信、彩信、邮件。尽量避免将手机应用账户设置为自动登录，同时为手机设置锁屏密码及开机密码。

    其次，通过正规渠道下载手机软件。登录官方平台或安全可靠的应用市场如360手机助手等下载。不要使用来路不明的软件，不要浏览不良网页。安装软件时，一定要详细查看软件索取的权限列表，出现敏感权限时要特别警惕。



    再次，遇有手机异常及时使用360手机卫士等安全软件查杀。并养成定期为手机体检扫描恶意程序的好习惯。

**1分钱兑换话费？360提醒小心支付宝被“钓鱼”**

    “支付宝周年活动，一分钱换50元话费！”如果有人在QQ或QQ空间上给你发来这样的中奖链接，可一定要当心了。360手机卫士根据网友反馈分析，这是近期频繁出现的最新诈骗手法，大量用户点进去输入支付宝账号和密码不仅没有兑换到话费，自己的支付宝反而被盗刷130元。



    有网友反馈，自己12日下午收到了一条QQ消息，称支付宝正在进行10周年活动，可以一分钱兑换50元话费，并发来了一个网址链接。点击链接后，根据网页提示填写了手机号码，并转入支付宝付款一分钱的页面。在按要求输入支付宝密码与验证码后，不仅没收到50元话费，查询支付宝账户发现反被扣款130元。



    360手机安全专家介绍，这是典型的支付宝话费中奖欺诈。根据360手机卫士统计数据显示，进入暑期，此类诈骗变得十分频繁。不法分子主要针对消费能力较低、安全意识较为薄弱的学生群体，盗取QQ号后借助QQ和QQ空间散播钓鱼链接，一旦有用户信以为真点击链接就有可能掉入陷阱。目前，360手机卫士可以全面拦截此类钓鱼网站。



    对此，专家提醒，面对噱头十足的中奖信息，千万不要贪图便宜，一定要保持头脑冷静，不要盲目在安全性不明的网页填写银行卡号，密码等敏感信息。其次，不要点击不明链接，不要扫描陌生二维码，在网络上进行付款等交易行为时，一定要使用360手机卫士等安全软件，鉴别和拦截钓鱼网站；最后，要定期更新网上交易的账号和密码，尽量避免将虚拟银行和现实中的借记卡挂钩，保护资金安全。

  **骗子新招数！“有人冒充你在外地申请了护照”**

    层出不穷的电话诈骗已经让人防不胜防，昆明市公安局最近接到多名市民反映，有人冒充出入境部门，欲骗取市民个人信息。360手机安全专家指出，此类诈骗电话今年已出现多起，手机用户如接到自称“出入境”工作人员的电话时务必多加留心，当对方提到银行卡号等敏感信息时，更要提高警惕。



    “有人冒充你在外地申请了护照，请配合我们调查……”多位昆明市民接到了这样的电话，被对方的身份所震慑，由于来电显示为当地出入境管理部门的官方电话，且对方在电话中明确说出受害者的姓名及身份证号码等信息，让受害者确信无疑。



    骗子还进一步表示，有人利用受害者的出境证件，在境外从事非法洗黑钱活动，要求受骗者配合调查，不然将限制出境，并冻结账户。随后，便要求受害者提供个人银行账号等信息。360手机安全专家指出，这是骗子利用改号系统冒充相应机关单位骗取市民个人信息。据了解，去年电信诈骗案发40万余起，比2013年增长34%。

    据360手机安全专家介绍，通过在正常通讯网络之间的协议里篡改信息，骗子可以将主叫号码设置成任意号码，包括银行客服电话、运营商服务电话，甚至是政府部门、执法机关等一些“官方号码”。而且改号软件只是实施诈骗的第一步，其目的是利用伪装后的电话号码，骗取用户的信任，并趁机向用户发送设置好的钓鱼网站链接，当用户依照骗子的指示登录钓鱼网站输入个人信息，骗子们便“大功告成”。



    针对此类诈骗，360手机安全专家提醒，在接到公检法机关、出入境管理机关或各种金融、电信、邮政的电话时不要轻信，可自行拨打官方的客服电话进行核实确认，因为去电号码无法被随意更改；同时，建议手机用户下载安装360手机卫士等手机安全软件，使用骚扰拦截功能，对手机进行实时防护，当有陌生短信或电话过来时，可通过360手机卫士进行自动识别。

    除此之外，安全专家还建议，网民需增强个人信息保护意识，遇到可疑人员以出入境管理事务为由索要个人重要信息，特别是要求提供银行账号、转账的，一定要提高警惕。