



# 保护网络信息安全多方“亮剑”

本报记者 陈 静

**导读：**截至2012年6月底，我国网民数量已达到5.38亿。庞大的数字，既带来了创新生活方式和消费模式的勃勃生机，也让网络信息安全保护成为焦点话题。来自互联网安全厂商的数据显示，网络犯罪每年给我国网民造成的经济损失达2890亿元，其中仅钓鱼网站这一项带来的损失就将近300亿元。同时来自市场研究机构易观的调查显示，安装杀毒软件并定期升级更新的网民比例仅有32%，在网络支付用户中安装“数字证书”的用户仅占14.9%。

在这样的大背景下，一方面加强网络信息保护立法有望有效地减少网络犯罪，降低经济损失；另一方面，也需要移动运营商、社交网站、电子商务企业和互联网安全厂商等携手努力，在保护网络信息安全方面“多管齐下”。目前这些企业在保护网络信息安全方面进行了哪些工作？存在哪些难点？普通网民又该采取哪些手段自我保护？本期“新视野”将为您解答这些问题。

## 实名制需要长效机制

28岁的福建姑娘周冲霄大学毕业后不久，在淘宝上开了个专卖饰品的网店，她给记者看了两张照片，一张是她拿着自己身份证的大头照，一张是上半身照。“这是我拿去淘宝网作实名认证用的。”从今年6月30日起，没有通过实名认证的淘宝网店铺就会被屏蔽。

作为政协委员，神州数码董事局主席郭为在今年的“两会”上专门提出保护网络信息安全,推行实名制的提案。他认为,从可用到可信,实名制被视为净化网络、打击网络欺诈、保护青少年的有效手段。除了网络购物,像开网站、百合网、世纪佳缘这样的社交网络和交友网站也纷纷全站“实名”。拿世纪佳缘子网站爱真心为例,所有用户注册时必须通过手机加身份信息认证注册。同时,世纪佳缘还联合权威机构为爱真心的用户提供视频、邮箱、学历、购车、财产等认证方式。在用户交友过程中,爱真心的信息审核系统会根据用户所有信息进行立体交叉式匹配,认证会员信息的真实性和有效性。

实名制应用领域的不断拓展,意味着普通人要更多地向外提供自己的个人信息。从2011年底的CSDN大规模网络泄密到今年的京东、当当等一系列账号泄密事件,以及网络泄密对韩国网络实名制的巨大打击,都让人们不禁有这样的疑问:如果全网推行实名制,又该如何保障信息安全?

互联网安全厂商瑞星的安全专家唐威表示,扩大实名制推行就必须有一套与之相匹配的长效机制。“首先,不同的网站类型都要采用统一的实名制实施对策;其次,对用户信息的存储,有关部门一定要出台规范的存储方法;第三,从软硬件角度同时着手,加强网站的安全建设和防护水平;第四,有关部门必须加强信息管理水平建设,排除‘内鬼’泄露用户信息的可能;第五,加大力度打击以窃取用户信息牟利的‘灰色产业链’。”

## 互联网企业“重拳”出击

面对严峻的网络安全形势,互联网服务提供商并非仅有实名制这一个“杀手锏”,他们也在根据自己的服务性质和应用种类,用技术和产品来为网民的信息安全“保驾护航”。

《新浪微博社区管理规定》中明确规定,通过伪造材料,提供虚假信息,获取新浪微博



用户正登录社交网站人人网查看好友们的动态。作为人数增长最快的互联网应用之一,社交网站在网络信息保护方面任重道远。 陈 静摄

个人认证身份,用户真实身份与个人认证身份不符属于违规行为,站方接受对“个人认证用户身份虚假”的举报。与此同时,一旦发现有用户发布垃圾广告,该用户就会被直接删除账号。搜狐副总裁国庆临介绍说,目前搜狐微博建立了好几道防火墙以应对不良信息的控制。“首先是系统过滤,如果内容触及了敏感词汇就会进入系统通过微博自律专员进行人工审查。”国庆临表示。在这之外,利用微博传播的互动性、即时性等特点,搜狐微博还构建了一道“全民防火墙”,那就是“网络评审员制度”和“网友举报平台”。虚假信息一旦查实后,就会将“犯案微博”删除。

网络购物平台则直接事关网民口袋中“真金白银”的安全。腾讯电商称,一直非常重视用户个人电子信息保护,依托腾讯公司的安全保护措施保护用户的账号安全。具体来说主要有两个方面:第一,不会主动收集用户信息;第二,用户在腾讯电商平台进行交易的账户信息全部储存在保护区,设置了多层权限控制,并且账号密码等敏感信息采用加密存储。支付宝安全副总裁江朝阳则向记者介绍说,从

技术上讲,为了保障用户的密码安全,支付宝推出了专门的密码安全控件。该安全控件对用户的关键信息进行再次多重加密,能够有效防止账户密码被木马程序或病毒窃取,无人可通过密文获得用户密码。如果用户账户被盗,交易出现异常操作,支付宝的风险控制系统能够根据规则,及时主动进行判定,采取措施,包括要求对方输入绑定手机接收到的动态口令甚至直接阻止交易等,从而降低损失风险。

## 安全厂商瞄准细分市场

尽管大型互联网服务提供商们各出奇招,但还需要使用专业的互联网安全产品进行应对。互联网安全厂商们注意到互联网首要安全问题从“病毒破坏”到“窃取信息”的变化,并随之深耕细分市场。

瑞星主打“企业牌”。唐威介绍说,单独窃取个人用户信息成本较高,所以黑客通常选择针对企业下手,比如针对某一个电商网站,或者针对微博和邮件服务商。瑞星刚刚发布的企业终端安全管理系统就可以为这样的企业提

供整体解决方案。“在这个方案里对所有跟安全相关的行为都有相应管理措施,比如这个方案中的‘堡垒主机’,它可以对整个运维管理和服务器进行全面、全程监控,因为用户的信息都存在服务器里,就可以避免‘内鬼’私下拷贝和贩卖这些信息。”

腾讯和金山则瞄准了移动互联网。腾讯无线安全产品部总经理胡振东在接受采访时表示:“腾讯手机管家通过权限监控、程序锁定、照片、视频、通信、文件等功能设定全方位加密保护。”金山手机毒霸在本月新推出了“聪明的软件隐私权限管理”,让用户看得懂隐私权限说明、不关错隐私权限。比如为什么YY语音需获取位置信息,访问通讯录等权限?手机毒霸可在扫描结果中告诉用户,相应权限分别是为“测算与好友的距离”、“添加联系人为YY好友”等等,即使是毫无智能手机使用经验的用户,也能一眼看懂。此外,手机毒霸还推出了“广告分级制”,明确区分恶意广告、风险广告和正常广告,用户均可根据需求进行精准管理。这一举动旨在保护用户利益,对合法开发者广告商提供安全背书,支持行业健康发展。

# 搜索引擎:有效过滤不良信息

龚 玺

搜索引擎作为社会大众获取信息的重要渠道,给人们的日常生活和工作带来了便利,同时也给我们的个人信息安全带来了隐患和威胁。有国外安全厂商做过调查发现,有75%的网络钓鱼组织通过搜索引擎来寻找存在漏洞的站点,并对所找到的站点进行网络钓鱼攻击。

搜索中的数据挖掘技术,常常用来做精准营销,但也是泄露个人隐私的途径之一。在事业单位工作的小谭在搜索网页上输入“智能手机”,有关智能手机的信息便集中展现出来,网站也“记住”了他对智能手机感兴趣,以后凡有智能手机的消息就会推送给他。正是由于个人信息的被搜集、加工、集成,从而属于个人隐私的权益极易被侵害。有的数据挖掘技术还可能会访问到有密码保护的内容,威胁个人信息安全。

纵观目前的搜索市场,各主流厂商都加大了对信息安全和不良信息的管控。如奇虎360日前发布的“网站照妖镜”就是针对钓鱼网站推出的一款安全产品,保障用户搜索不上当、网购不丢钱、上网不受骗。谷歌和百度也都有相应产品,以防止网民信息安全泄露。

“第三代搜索技术正在兴起,其更加注重信息安全。”业界专家表示,第三代搜索是多方知识的融合,其信息安全技术处于业内领先水平。特别是在用户行为跟踪方面,大部分网站会对网友行为进行收集及分析,比如“我的空间”谁来过,谁留过言等,借助这些浏览痕迹推动网友间的互动。然而,这一服务却成为信息安全的隐患。

有些搜索引擎平台,出于保护用户隐私的目的,选择屏蔽用户行为跟踪。中搜研发的第三代搜索引擎突破了固有模式,把选择权交给

网民。关注自身隐私的用户可以在第三代搜索中选择隐藏自己的浏览路径,而希望被更多人关注的用户则可以选择保存浏览路径。

据介绍,全新的第三代搜索引擎,采用的是开放性搜索模式,用户可以参与到搜索结果的编辑制作中来,生成更加符合用户需求 and 个性化的搜索结果。这种开放的搜索引擎将对传统搜索模式产生颠覆性的影响,搜索也更安全。此外,“第三代搜索的所有结果都以链接的方式呈现,网民不可能通过第三代搜索跳过信息提供网站,所以也就不存在对第三方网站的利益侵蚀”。中搜总裁陈沛介绍说,从中搜自己的产品来看,中搜有着一套较成熟的识别体系和安全体系。“所有泄露个人隐私、危害互联网信息安全的行为都能通过机器和人工筛查检测出来,从而有效阻止了影响信息安全的隐患。”

投诉举报,并配置专人专岗处理客户举报信息,确保举报信息及时有效处理。

工业和信息化部为保护网络信息安全建立的“12321”举报中心功能则更加强大。可以举报包括互联网网站、论坛、电子邮件、即时消息、博客、手机、固定电话、传真等传播、发送的不良与垃圾信息。

受访电信运营商表示,尽管在加强网络信息保护、垃圾短信治理工作方面取得了一定成效,但仍存在一些突出问题亟待解决。

一是法律层面上对于垃圾短信无明确定义,对群发垃圾短信的人员没有相应的判罚条款,在零处罚与高回报的利益驱动下,一些人便肆无忌惮,这也就是运营商一直在大力治理,却无法有效杜绝的根本原因。二是系统拦截能力有限,群发商利用电脑控制群发器采用连续低频和变换短信格式的方式发送短信,在现有技术水平下,存在一定的误拦和漏拦,对于短信误拦和漏拦都会引起用户的投诉,由于相关法律法规的缺失,行业内没有统一的处置标准和解释口径,使得尽管运营商一直在努力履行社会义务,却仍处在十分被动的局面。三是垃圾短信给运营商带来巨大经济损失,一些不法分子利用复制卡或其他技术漏洞群发垃圾短信,产生大量欠费和高额网间结算支出,这些损失是很难追回的。

# 十招教您安全上网

本报记者 陈 静 谭 辛

网民如何在实用互联网和移动互联网服务时进行自我保护?其实,一些简单的技巧就可以帮您大大减少在网上泄露个人隐私和遭遇其他风险的几率。记者采访了移动运营商和互联网安全厂商的安全专家们,请他们为您支上几招。

1、**安装安全软件。**在电脑和手机上都要安装功能全面的专业安全软件产品,它不但能够对用户隐私进行加密,还能对黑客有很好的拦截防御作用。

2、**注册网站账号有技巧。**不要觉得大网站就一定能够保护好自己的密码,因此不要随意注册网站账号,用户名、账号和密码尽量每个网站各不相同,并使用随机数字,同时应定期更换密码。

3、**不轻易在不知名的电商网站购物。**如果有必要购物,可以采用“货到付款”的方式,送货地址可以填写公司地址(不要填写家庭地址)。

4、**常用网站可以将账号与手机绑定。**这样绑定之后,一旦有账号变动异常,用户会及时收到消息,降低损失。

5、**不要轻易点开短链接。**微博的字数限制让短链接被人们所熟悉。但它也很容易被木马或者钓鱼网站利用,诱骗用户点击。用户可将鼠标放置在短链接上,即可看到完整网址。

6、**养成良好的上网习惯。**其中,在使用互联网应用产品或者服务时,一定要仔细看一下它的用户许可协议或者是隐私条例,定期修复第三方软件漏洞以及系统漏洞,使用聊天工具时不轻易打开好友发来的链接。

7、**尽量不破解手机的操作系统。**诸如苹果手机的“越狱”或者安卓手机的“刷机”,其实都是打开了手机的最高权限,这样下载来的程序就可以在手机上为所欲为。

8、**手机数据交换要小心谨慎。**使用SD卡、T-FLASH等内存卡交换数据时先杀毒,隐藏或关闭手机的蓝牙功能,以防手机自动接收病毒。

9、**切勿随便登录WIFI无线上网热点。**不法分子极易通过伪装成公共的免费WIFI热点扩散手机病毒,导致使用者个人信息的泄露。所以,在提供免费WIFI上网咖啡馆、餐厅等场所上网时,一定要事前问清用户名。

10、**对手机短信提高警惕。**不信、不汇款、不转账的预防措施。当手机用户收到一些短消息实在难辨真伪时,最好咨询本地运营商的客户电话、消费者协会、警方,或及时与家人、朋友沟通。

## 新年临近

## 电商促销忙

新年假期前,电商网站们又掀起了新一轮促销高潮,各大平台的负责人出现在分拣配送一线,吸引了网民的大量眼球。



疯狂促销使得近期几家诚品的订单激增,拣货量是平时的5倍左右。各地积压订单接近100万单。图为12月25日,凡客诚品CEO陈年亲自上阵充当仓库拣货员。未来半个月,包括陈年在内的所有管理团队,都将继续在一线奋战。 李 娜摄



腾讯旗下电商平台易迅网CEO卜广齐亲自上阵送货。25日当天,易迅网CEO卜广齐扮成圣诞老人送货,让人联想起京东商城CEO刘强东骑电动车送货的场景。易迅网无论在营销方式还是价格竞争方面都在逼近着京东商城,看来明年这两家网站在3C领域的竞争还将会愈演愈烈。 吴 铭摄

本版编辑 徐 红

# 运营商积极加强网络信息保护

本报记者 谭 辛

据工业和信息化部“12321网络不良与垃圾信息举报受理中心”数据统计,2012年上半年,我国手机短信用户平均每周收到垃圾短信息10.6条,环比下降了0.8条,下降7.0%,同比下降2.4条,下降18.5%。收到垃圾短信息占全部短信息的比例为22.1%,环比下降0.5个百分点,同比下降5.2个百分点。

电信专家指出,保护信息安全,特别是客户信息安全是电信企业应承担的社会责任。从数据来看垃圾短信的数量有下降的趋势,垃圾短信的治理工作取得了一定的效果。同时,表现出国内电信运营商开展了一系列保护信息安全的综合治理工作。

“目前,中国电信不但建立起集团公司、省公司、专业公司(增值业务中心)三级联动的投诉处理流程,还把垃圾短信治理工作纳入到中国电信集团责任部门和各省公司的绩效考

核KPI考核指标中,建立常态化工作机制,在体制机制上遏制垃圾短信泛滥的势头。”中国电信客服部总经理朱正武说。中国电信将用户个人信息保护视为一项重要的基础性工作,融入企业的经营管理全过程,制定了《中国电信代理商管理规范》。

截至今年4月上旬,中国电信基本完成对行业短彩信业务、自营类行业短彩信业务、SP合作类短彩信业务等端口群发短信业务的客户资料复核和业务清查工作,累计复核客户76897家,关停了其中24822家。

“为维护用户合法权益和正常通信秩序,在技术方面,中国联通在全国31个省区市均部署了垃圾短信拦截系统,进一步加大人工审核力度,规范行业应用端口管理,并及时根据拦截情况优化拦截策略,提高精准度。”中国联通集团公司综合部处长温宝球介绍,目前,

中国联通按照“谁接入,谁负责”的原则,严格控制短信下发内容、时间和范围,提高处罚标准;完善拦截技术手段,建立拦截策略全国共享机制,确保人工审核人员编制,据用户属性区分流控频次,实行精准拦截。

中国移动则着力推动信息安全工作从“事后处理”向“事前预防”、“事中监督”转变。2011年11月,中国移动成立了信息安全管理与运行中心,负责不良信息治理和信息安全工作的统筹协调和归口管理。2012年9月,中国移动(洛阳)信息安全运营中心启用,配备360名专业人员,开展集中发现和处置垃圾短信,是当前我国运营商中规模最大的信息安全集中运营团队。中心启用以来,日均处理不良信息约59万件,极大提高了不良信息发现处置效率。此外,中国移动建立10086热线、10086999短彩信举报平台、门户网站等多个免费举报渠道,接收客户