国家网络安全宣传周
China Cybersecurity Week

共建网络安全 共享网络文明

第二届国家网络安全宣传周

2015年6月1日-7日

网络安全知识笔记

共建网络安全 共享网络文明

第二届国家网络安全宣传周

联合主办单位：

中央网络安全和信息化领导小组办公室

中央机构编制委员会办公室

教育部

科技部

工业和信息化部

公安部

中国人民银行

国家新闻出版广电总局

中国共产主义青年团中央委员会

中国科学技术协会

协办单位：北京市委网络安全和信息化领导小组办公室

承办单位：工业和信息化部电子科学技术情报研究所

一、国家网络安全宣传周

2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立并召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出保障网络安全、维护国家利益、推动信息化发展的决心。习近平总书记在会议上强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局、统筹各方、创新发展，努力把我国建设成为网络强国。会议审议通过了《中央网络安全和信息化领导小组 2014 年重点工作》，其中提出设立国家网络安全宣传周。通过宣传周加强网络安全宣传教育，引导社会公众共同维护网络安全。

二、首届国家网络安全宣传周回顾

2014 年 11 月 24 日至 30 日，首届国家网络安全宣传周成功举办。中共中央政治局常委、中央书记处书记、中央网络安全和信息化领导小组副组长刘云山出席启动仪式并发表重要讲话，充分体现了党中央对网络安全工作的高度重视，极大激励和鼓舞了社会公众，掀起了全民讨论、参与网络安全的热潮。

首届宣传周由中央网信办、中央编办、教育部、科技部、工业和信息化部、公安部、中国人民银行、新闻出版广电总局 8 个部门联合主办，设置了启动日、政务日、金融日、产业日、电信日、青少年日、法治日 7 个主题宣传日，开展了公众体验展、公益短片征集展映、网络安全知识大讲堂、网络安全知识手册发放等各类主题宣传活动 25 项，累计达上千场次。期间，发放知识手册 1500 余万册，征集到 94 部公益短片在线点击量达 500 万次，七天公众体验展参观总人数超过 5.3 万。300 多家主流媒体展开了全方位、多角度的深入报道，各类网络媒体刊发相关消息 2760 万篇次。全国各省（自治区、直辖市）同步开展了主题宣传活动。

院士专家、企业、广大民众通过各种方式，为网络安全宣传贡献力量。多

名院士出席启动仪式或致电表达对宣传周的支持与肯定。数百名专家为宣传周出谋划策，并通过发表署名文章、接受媒体采访等方式，大力传播网络安全理念。由互联网巨头、知名网络安全公司、重点金融机构、电信运营商等组成的 49 家参展企业投入大量人力和物力，精心布展、巧妙构思，让参观者能够亲身体验常见网络安全风险。广大民众也纷纷加入宣传大军，宣传周期间与“网络安全”相关微博达 51 万条、微信达 10.3 万条。

三、第二届国家网络安全宣传周介绍

为进一步加强全党全社会网络安全意识，发动全社会参与维护网络安全，中央网信办、中央编办、教育部、科技部、工业和信息化部、公安部、新闻出版广电总局、中国人民银行、共青团中央、中国科协 10 个部门于 2015 年 6 月 1 日至 7 日联合举办第二届国家网络安全宣传周，全国各地同步开展。

第二届宣传周沿用首届“共建网络安全 共享网络文明”主题，传播“安全方面最大的风险是没有意识到风险”的理念，重点加强青少年网络安全教育。

线下活动包括启动仪式暨国家网络安全青少年科普基地揭牌仪式、“赢在未来”青少年网络安全教育联合行动、“感知身边的网络安全”公众体验展、“争做网络安全卫士”系列青少年网络安全知识竞赛、“网络安全知识大讲堂”知识讲座、“网络安全知识进万家”知识手册发放等。

线上活动包括“讲述身边的网络安全故事”文章和微电影征集展映、在线网络安全知识竞答、我国首次“公众网络安全意识调查”、专家访谈等。中央新闻网站和重点商业网站将设立宣传周专题，推出新闻评论、嘉宾访谈等原创网络安全宣传内容。

宣传周设立启动日、金融日、电信日、政务日、科技日、法治日、青少年日 7 个主题日，联合主办各部门依据职能在相应主题日组织开展集中宣传活动。同时，鼓励支持各类社会团体、专业机构，深入开展网络安全知识普及、网络安全防护技能培训等活动。

更多详情，敬请关注宣传周官网 :http://wlaqz.cac.gov.cn

计算机安全防护

在使用电脑过程中应该采取哪些网络安全防范措施

1. 安装防火墙和防病毒软件，并经常升级，及时更新木马库 , 给操作系统和其他软件打补丁。
2. 对计算机系统的各个账号要设置口令，及时删除或禁用过期账号。
3. 不要打开来历不明的网页、邮箱链接或附件，不要执行从网上下载后未经杀毒处理的软件，不要打开 QQ 等即时聊天工具上收到的不明文件等。
4. 打开任何移动存储器前用杀毒软件进行检查。
5. 定期备份，以便遭到病毒严重破坏后能迅速修复。

计算机安全防护

如何将网页浏览器配置得更安全

1. 设置统一、可信的浏览器初始页面。
2. 定期清理浏览器缓存的临时文件、历史记录、Cookie、保存的密码和网页表单信息等。
3. 利用病毒防护软件对所有下载资源进行及时的恶意代码扫描。

计算机安全防护

如何防范 U 盘、移动硬盘泄密

1. 及时查杀木马与病毒。
2. 从正规商家购买可移动存储介质。
3. 定期备份并加密重要数据。
4. 将 U 盘、移动硬盘接入电脑前，先进行病毒扫描。

计算机安全防护

计算机中毒后有哪些症状

1. 经常死机。
2. 文件打不开。
3. 经常报告内存或硬盘空间不够。
4. 出现大量来历不明的文件。
5. 数据丢失。
6. 系统运行速度慢。
7. 操作系统自动执行操作。

应用安全防范

如何防范 QQ、微博等账号被盗

1. 账户和密码不要相同，尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码。
2. 针对不同用途的网络应用，应该设置不同的用户名和密码。
3. 在多人公用的计算机上登录前重启机器，警惕输入账号密码时被人偷看。

应用安全防范

如何安全使用电子邮件

1. 不要随意点击不明邮件中的链接、图片、文件。
2. 适当设置找回密码的提示问题。
3. 当收到与个人信息和金钱相关（如中奖、集资等）的邮件时要提高警惕。

应用安全防范

如何防范社交网站信息泄露

1. 利用社交网站的安全与隐私设置保护敏感信息。
2. 不要轻意点击未经核实的链接。
3. 在社交网站谨慎发布个人信息。

应用安全防范

如何保护网银安全

1. 尽量不在多人公用的计算机上使用网银，发现异常时及时修改密码并向银行求助。
2. 核实银行的正确网址，并使用银行提供的数字证书。
3. 设置复杂度高的网银登录和支付密码，登录时不要“记住密码”，尽量使用软件盘输入账号及密码。
4. 交易完成后及时退出并拔下 U 盾。
5. 对网络单笔销费和转账进行金额限制，并开通短信提醒功能。

应用安全防范

如何保护网上购物安全

1. 核实网站资质及联系方式的真伪，要到知名、权威的网上商城购物，不要轻信网上低价推销。
2. 尽量通过网上第三方支付平台交易，并检查支付网站的真实性，切忌直接与卖家私下交易。
3. 购物时要注意商家的信誉、评价和联系方式。
4. 交易完成后完整保存交易订单等信息。
5. 直接使用银行账号、密码和证件号码等敏感信息时要慎重。

应用安全防范

如何保护网上炒股安全

1. 尽量不在多人共用的计算机上进行股票交易，并注意在离开电脑时锁屏。
2. 核实证券公司的网站地址，下载官方提供的证券交易软件，不要轻信小广告。
3. 及时修改个人账户的初始密码，设置安全密码，发现交易有异常情况，要及时修改密码，并通过截图、拍照等保留证据，第一时间向专业机构或证券公司求助。

应用安全防范

如何在使用网络地图时维护地理信息安全

1. 在使用互联网地理信息服务时，主动了解国家地理信息安全的法律规定。
2. 不上传标注涉密和敏感地理信息，如军用机场、导弹阵地、雷达阵地、海军港口、部队驻地等重要军事目标，以及石油、电力、燃气等涉及国家经济命脉的大型公共服务设施等。
3. 对发现的网络地理信息失泄密行为，及时向相应测绘地理信息行政主管部门举报。

网上陷阱识别

如何防范网络谣言

1. 注意辨别信息的来源和可靠度，通过经第三方可信网站认证的网站获取信息。
2. 不造谣、不信谣、不传谣。
3. 及时举报疑似谣言信息。

网上陷阱识别

如何防范网络诈骗

1. 不贪便宜，仔细甄别，严加防范。
2. 使用安全的支付工具。
3. 不在网上购买非正当产品，如手机监听器、毕业证书、考题答案等。
4. 不要轻信以各种名义要求你先付款的信息，不要轻易把自己的银行卡借给他人，不向他人透露本人证件号码、账号、密码等。

网上陷阱识别

如何防范钓鱼网站

1. 通过查询网站备案信息等方式核实网站资质的真伪。
2. 注意防护软件弹出的警告和提示信息。
3. 要警惕中奖、修改网银密码的通知邮件、短信，这很可能是钓鱼网站设置的陷阱。

网上陷阱识别

如何准确访问和识别党政机关、事业单位网站

1. 通过“.政务”和“.公益”等中文域名访问党政机关、事业单位网站。

2. 通过查看党政机关和事业单位两类网站标识识别，该标识位于网站所有页面底部中间显著位置。

网上陷阱识别

如何防范网络传销

1. 在遇到相关创业、投资项目时，一定要仔细研究其商业模式。如果其经营的项目并不创造任何财富，请提高警惕。
2. 克服贪欲，不要幻想“一夜暴富”。

网上陷阱识别

网上受骗后该如何减少自身的损失

1. 及时致电发卡银行客服热线或直接向银行柜面报告欺诈交易，监控银行卡交易或冻结、止付银行卡账户。
2. 对已发生损失或情况严重的，应及时向当地公安机构报案。
3. 配合公安机关或发卡银行做好调查、举证工作。

移动终端安全

如何安全地使用 Wi-Fi

1. 关闭设备的无线网络自动连接功能，仅在需要时开启。
2. 警惕公共场所免费的无线信号，应特别注意与公共场所内已开放的 Wi-Fi 名称类似的信号很可能是钓鱼陷阱，尽量不要在公共场所进行网银操作。
3. 修改家中无线路由器默认用户名和密码；启用 WPA/WEP 加密方式；修改默认 SSID 号，关闭 SSID 广播；必要时可启用 MAC 地址过滤；无人使用时，关闭路由器电源。

移动终端安全

如何安全地使用智能手机

1. 设置锁屏密码。
2. 不要轻易打开陌生人发送至手机的链接和文件。
3. 在 QQ、微信等应用程序中关闭地理定位功能，仅在需要时开启蓝牙。
4. 经常备份手机数据。
5. 安装手机安全防护软件，经常对手机系统进行扫描。
6. 不要见 Wi-Fi 就上，见码就刷。
7. 到权威网站下载手机应用软件，并在安装时谨慎选择相关权限。
8. 不要试图破解自己的手机。

移动终端安全

如何防范“伪基站”的危害

1. 当用户发现手机无信号或者信号极弱时仍然收到了推广、中奖、银行等相关短信，则用户所在区域很可能被“伪基站”覆盖，不要相信短信的任何内容。
2. 不要轻信任何号码发来的涉及银行转账及个人财产的任何短信，不向任何陌生帐号转账。
3. 安装手机安全防护软件，以便对收到的垃圾短信进行精准拦截。

移动终端安全

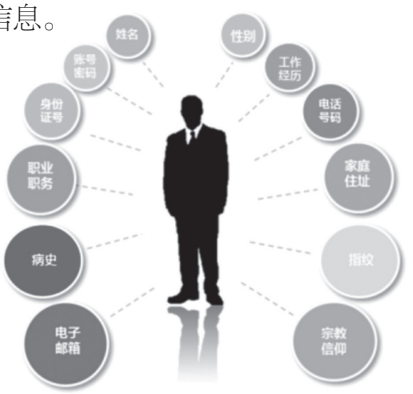
如何保护手机支付安全

1. 随身携带手机，建议手机支付客户端与手机绑定，使用数字证书，开启实名认证。
2. 从官方网站下载手机支付客户端和网上商城应用。
3. 使用手机支付服务前，按要求安装专门用于安全防范的插件。
4. 登录手机支付应用、网上商城时，勿选择“记住密码”选项。
5. 经常查看手机任务管理器，检查是否有恶意程序运行，并定期扫描系统。

个人信息保护

如何防范个人信息泄露

1. 在安全级别较高的物理或逻辑区域内处理个人敏感信息。
2. 个人敏感信息需加密保存。
3. 不使用 U 盘存储交互个人敏感信息。
4. 尽量不要在可访问互联网的设备上保存或处理个人敏感信息。
5. 只将个人信息转移给合法的接收者。
6. 个人敏感信息需带出时要防止被盗、丢失。
7. 电子邮件发送时要加密，并注意不要错发。
8. 注意存有个人信息的纸质资料的存储、传输及销毁。
9. 废弃的光盘、U 盘、电脑等要消磁或彻底破坏。



个人信息保护

网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人信息，应当遵循什么原则

应当遵循合法、正当、必要的原则，明示收集和使用信息的目的、方式和范围，并经被收集者同意；不得违反法律、法规的规定以及双方的约定收集和使用公民个人信息。

个人信息保护

当公民个人发现网上有泄露个人身份、侵犯个人隐私的网络信息该怎么办

公民发现泄露个人身份、侵犯个人隐私的网络信息，或者受到商业性电子信息侵扰，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止，必要时可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。公民还可依据《侵权责任法》《消费者权益保护法》等，通过法律手段进一步维护自己的合法权益，如要求侵权人赔礼道歉、消除影响、恢复名誉、赔偿损失等。

法律法规知识

即时通信工具（如微信、腾讯 QQ 等）使用者注册账号时应承诺遵守哪些规定

国家互联网信息办公室 2014 年 8 月 7 日发布《即时通信工具公众信息服务发展管理暂行规定》，明确要求即时通信工具服务使用者注册账号时，应当与即时通信工具服务提供者签订协议，承诺遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等“七条底线”。

法律法规知识

除哪些情形外，利用网络公开自然人个人隐私造成他人损害的，需承担侵权责任

《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》明确以下情形除外：

（一）经自然人书面同意且在约定范围内公开。

（二）为促进社会公共利益且在必要范围内。

（三）学校、科研机构等基于公共利益为学术研究或者统计的目的，经自然人书面同意，且公开的方式不足以识别特定自然人。

（四）自然人自行在网络上公开的信息或者其他已合法公开的个人信息。

（五）以合法渠道获取的个人信息。

（六）法律或者行政法规另有规定。

法律法规知识

在互联网信息服务中注册或使用的账号名称不得出现哪些情形

2015 年 2 月 4 日，国家互联网信息办公室发布《互联网用户账号名称管理规定》，明确要求任何机构或个人注册和使用的互联网用户账号名称，不得有下列情形：

（一）违反宪法或法律法规规定的。

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

（三）损害国家荣誉和利益的，损害公共利益的。

（四）煽动民族仇恨、民族歧视，破坏民族团结的。

（五）破坏国家宗教政策，宣扬邪教和封建迷信的。

（六）散布谣言，扰乱社会秩序，破坏社会稳定的。

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

（八）侮辱或者诽谤他人，侵害他人合法权益的。

（九）含有法律、行政法规禁止的其他内容的。

法律法规知识

网上的哪些行为被认定为《刑法》第二百四十六条第一款规定的“捏造事实诽谤他人”

1. 捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的。
2. 将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的。

   明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

法律法规知识

现行《刑法》中，专门规定了哪两个关于计算机犯罪的罪名

【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

法律法规知识

禁止从事哪些危害计算机信息网络安全的活动

《计算机信息网络国际联网安全保护管理办法》规定，任何单位和个人不得从事：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的。

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的。

（四）故意制作、传播计算机病毒等破坏性程序的。

（五）其他危害计算机信息网络安全的。

宣传周官网

宣传周官方微信

第二届国家网络安全宣传周