国家网络安全宣传周
China Cybersecurity Week

2020年商洛市第七届国家网络安全宣传周宣传手册

7th

中共商洛市委网信办
商洛市互联网信息办公室
2020年9月

网络安全为人民
网络安全靠人民

前 言

2020年国家网络安全宣传周将于9月14日-20日举行，主题是“网络安全为人民，网络安全靠人民”，全国各省（直辖市、自治区）同步开展。

商洛市第七届国家网络安全宣传周由商洛市委宣传部、商洛市委网信办、商洛市教育局、商洛市公安局、商洛市总工会、共青团商洛委员会、商洛市妇女联合会、中国人民银行商洛支行等八部门联合举办。将深入宣传《网络安全法》、《密码法》及相关配套法规，开展相关宣传活动，编写发放宣传资料，推动媒体、企业、社会团体广泛开展宣传普及，推进关键信息基础设施保护、大数据安全、个人信息保护等工作，通过展览、论坛、知识竞赛等多种形式，以及报刊、电台、电视台、网站等传播渠道，普及网络安全知识，提升全社会网络安全意识和防护技能。

“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全和信息化已经成为事关国家安全、政权安全和国家发展的重大战略问题，要求我们必须贯彻以人民为中心的发展思想，本着对社会负责、对人民负责、对国家负责的态度，发展好网信事业、治理好网络空间、守护好这个亿万民众共同的精神家园，让互联网更好地造福人民。

中共商洛市委网信办
商洛市互联网信息办公室

宣

商洛市第七届国家网络安全宣传周活动介绍

一、活动时间

2020年9月14日—20日

二、活动主题

网络安全为人民　网络安全靠人民

三、举办单位

商洛市委宣传部、商洛市委网信办、商洛市教育局、商洛市公安局、商洛市总工会、共青团商洛委员会、商洛市妇女联合会、中国人民银行商洛支行

四、重要活动

开幕式、主题活动日、网络安全知识技能竞赛、网络安全大讲堂、网络安全应急演练、网络安全进基层

五、主题日活动

9.15 校园日
9.16 电信日
9.17 法治日
9.18 金融日
9.19 青少年日
9.20 个人信息保护日

目　录 CONTENTS

三、网络安全

上网安全

终端安全

桌面安全

四、个人信息安全

五、法律法规知识

网络安全热点

疫情下的网络安全

随着新冠疫情肆虐，全球经济、科技、政治格局与博弈规则重写，后新冠时代新基础建设与科技创新带动经济复苏成为改变未来的重要力量。在此背景下，2020年两会期间科技界网络安全相关提案备受安全业界瞩目，因为无论新基建、数字化转型还是科技创新，对于网络安全行业来说都是一次前所未有的“颠覆性机遇”，这种颠覆性表现为：

1 信息技术从数字化转型的赋能者向技术创新的驱动者转型，网络安全市场迎来重大变革。

随着近年来网络攻击的组织化和复杂化，企业数字化转型和新基建面临新挑战，网络安全行业正在面临一次结构性的升级和变革，主要表现为：从被动防御到主动防御；从边缘安全到内生安全；“安全优先”，“安全左移”，从技术开发、架构设计和风险管理的早期阶段介入。

2 传统企业更加主动应对网络安全问题，安全和隐私保护能力正在成为企业数字化核心竞争力之一。

过去最顶尖的网络安全技术、人才、资本和实践主要是互联网科技公司，但是两会期间，一些传统企业高度关注网络安全和隐私保护话题，甚至主动针对网络安全法规、数据安全问题提案，表明网络安全已经成为传统企业数字化转型的焦点问题。

3 新基建需要全域化、全栈化的“大安全”。

新基建政府投资规模高达数十万亿，将深刻影响中国每一家企业，同时新基建的“安全设计”，也将对整个中国数字社会的“安全基因”产生重大影响。新基建作为数字经济的基础设施，其面临的网络安全风险和风险治理难度远高于企业网络，网络安全将从局部的、附属的、边缘的、伴生的技术投资项目，升级为云计算、5G、物联网、人工智能等新基础设施的“内生“、”全域“、“全栈”核心技术。

盘点两会网络安全热点

话题1：新基建

6000亿元预算，重点投资“两新一重”建设

“重点支持既促消费惠民生又调结构增后劲的‘两新一重’建设，主要是：加强新型基础设施建设，发展新一代信息网络，拓展5G应用，建设充电桩，推广新能源汽车，激发新消费需求、助力产业升级。”

—— 2020年《政府工作报告》摘要

1.网络安全是新基建最重要的基础性技术之一，必须要在新基建推进过程中同步部署。只有构建新基建网络安全防护体系，才能保障新基建战略的顺利推进和数字经济的健康繁荣。

具体建议如下：

（1）运用整体思维，规划新基建网络安全防护体系顶层设计；

（2）同步建设新基建的安全基础设施，聚焦新基建安全防能力构建；

（3）强化大数据平台安全，实现安全的大数据协同计算；

（4）开展常态化网络安全攻防对抗演习，持续检验和提升新基建安全能力。

2.在新基建网络安全建设中，要有宽广的视野。新基建下的网络形态不同于过往，网络边界可能更加模糊，相互之间的关联性会更强，因此不能囿于单一的点、线防护，要拓宽视野、更新思维，从深度和广度两方面加强工作，构建新型网络安全架构，提升对新形态下新威胁的认识和感知处置能力，形成广域、多层次的防护体系。

3.随着“数字基建”的推进，更多业务会以“网络+APP”形式来服务大众，网络安全的影响也就从原来的物理实体走向网络虚拟体，一旦出现网络安全问题，将给数字经济带来显著影响。在壮大网络安全产业的过程中，让更多有技术能力、有应用场景的企业和科研院所等参与到数字经济的网络安全建设中。把在不同领域、不同行业领先的安全能力变成国家网络安全能力体系的重要组成部分。出台数字经济“安全基建”标准，有关部门应尽快组织关于“安全基建”标准的调研，广泛了解企业在实践中积累且行之有效的做法，结合新一代信息通信技术发展情况，为构建完整的安全基础设施提供参考。

4.重视从源头构建安全能力的安全建设理念。网络安全不是事后应对的问题，而是事前提高“免疫力”的问题，要在广大企事业单位加强网络安全的教育和宣传，设定安全研发生产的红线。在数字基建的初始，就同步构建安全基础设施、提升风险免疫能力。

5.完善新基建安全体系建设。网络安全正在由过去的“辅助性”功能变成数字基础设施的重要一环，数字基建在建设伊始就要考虑安全体系的同步构建，从被动防控向主动防御转变。建议由国家互联网信息办公室牵头，联合工业和信息化部、公安部等有关部门，联动数字化程度较高的上游企业以及对安全体系、技术有深度研究的国立科研院所参与，产学研用全面结合，构建完整的安全基础设施。

话题2：发展工业互联网

“发展工业互联网，推进智能制造。电商网购、在线服务等新业态在抗疫中发挥了重要作用，要继续出台支持政策，全面推进“互联网+”，打造数字经济新优势。”

—— 2020年《政府工作报告》摘要

具体建议如下：

（1）加强工业互联网安全技术手段建设

出台工业互联网安全政策，提升安全行动力；加大国家资金投入，加快安全技术手段建设；多措并举强化产业支撑，推动完善产业生态。

网络安全热点

（2）推动人工智能赋能工业互联网安全发展

引导成立联合实验室促进技术研究与复合型人才培养；促进人工智能赋能工业互联网安全实践落地；推动人工智能赋能工业互联网安全可持续自适应演进。

话题3：个人信息保护

全国人大常委会工作报告在下一步主要工作安排中指出，围绕国家安全和社会治理，制定生物安全法、个人信息保护法、数据安全法，通过刑法修正案（十一），修改行政处罚法、人民武装警察法等。

具体建议如下：

（1）加强对疫情防控等特殊时期的个人信息保护

针对新冠肺炎疫情期间采集的个人信息设立退出机制，加强对已收集数据的规范性管理，研究制定特殊时期的公民个人信息收集、存储和使用的标准和规范。

（2）大数据应用背景下，保障个人信息安全迫在眉睫

加快立法进程。通过专门立法，统一对公私领域的个人信息保护，明确运营主体收集、使用个人信息的原则、程序和保密、保护义务，不当使用、保护不力的法律责任以及监管部门的监督手段和处罚措施等。

设立专门监管机构。建议在立法中明确专门机构负责或牵头负责个人信息保护工作，建立统一的制度规范，有权监督运营主体，并对违规行为进行处理。

确立运营主体运营规范。比如，要明确运营主体必须依法采集、使用、保管个人信息，有明确正当的目的，符合“最少、必需”要求，并经过信息主体明示同意；要加强从业人员管理，制定信息收集、处理、传输、公开、使用规则，做好流程监控，一旦发生信息泄露事件，严格追究相关人员责任。同时将技术防护纳入法律规范，推动运营主体加大技术防护投入。

赋予信息主体自我保护权力。比如，明确“信息自决权”，信息主体有权决定是否告知或允许他人利用自己的信息，建立“知情同意”制度，只有信息主体知情同意，运营主体方可采集、保管、使用个人信息；赋予“被遗忘权”，借鉴欧盟《通用数据保护条例》，信息主体行使“被遗忘权”时，运营主体不仅要删除自己所掌握的信息，还要对公开传播的信息负责，有义务通知其他人停止利用并删除。

话题4：数据安全

在第十三届全国人民代表大会第三次会议上，全国人大常委会工作报告指出：2020年将围绕国家安全和社会治理制定《个人信息保护法》、《数据安全法》等重要立法。

具体建议如下：

（1）强化数据安全专业立法和专项执法；

（2）积极开展数据和人工智能安全国际规则对接；

（3）加大扶持做大做强网络安全产业；

（4）建立适应人工智能发展的数据流通体系。

（5）细化数据安全与隐私保护规则，保护公民合法权益；

（6）明确数据的权利归属，促进数据的确权、流通、交易和保护；

（7）建立数据合理使用制度，实现个人与数据使用者之间的利益平衡；

（8）建立公共数据开放共享规则，促进公共数据的合理利用；

（9）完整确立我国数据跨境流动制度，应对国际数据竞争。

话题5：国家5G安全

“5G的价值并不简单地的是让我们手机看视频更快了，而是为我们整个产业互联网，整个物联网时代打造的。”作为新一代的数字基础设施，5G在赋能发展的同时也将引发新的网络安全风险，其安全性具有基础性和全局性意义。今年3月，工信部发布《关于推动5G加快发展的通知》，也明确表示，着力构建5G安全保障体系。

因此，应当从战略高度审视5G网络安全的重大意义和紧迫性，加强5G安全的顶层设计，制定《国家5G安全战略》。

话题6：物联网安全

推进智能车联网安全风险评估及检测。

具体建议如下：

（1）建议相关单位启动或加快完成车载网关、车载娱乐系统等信息安全标准制定；

（2）建议在《机动车运行安全技术条件》中增加信息安全要求，明确智能网联汽车、车辆辅助驾驶系统的信息安全风险评估要求和信息系统与数据安全要求；

（3）建议要求对含有电子系统、尤其是具有操作系统的智能网联汽车重要零部件进行销售前进行信息安全检测；

（4）建议包括无人试验车、无人出租车、低小慢速智能设备等智能网联车和含有辅助驾驶功能传统汽车、新能源汽车的在投入使用前必须进行全面的信息安全风险评估；

（5）建议要求针对无人试验车、无人出租车、低小慢速智能设备、电动车等智能网联车建立常态化的信息安全检测和评估机制；

（6）建议对全国在建或已建成的各无人车、智能网联汽车、低效慢速智能设备的示范区及封闭型试验区进行智能车联网络风险评估，并形成常态化评估机制；

（7）建议针对目前国内市场上所有的国外进口整车型号，根据《中华人民共和国网络安全法》和《个人隐私保护条例》等法律条例进行全面信息安全风险评估，并根据法律要求将云端车辆服务系统迁移至中国境内，以防止我国公民个人隐私信息的泄漏。

话题7：智慧城市

当前在建设智慧城市过程中，容易忽视的网络安全问题有以下几方面：

（1）缺乏智慧城市网络安全监管责任主体；

（2）智慧城市与信息安全发展关系亟须正确对待；

（3）智慧城市存在重大数据安全风险；

（4）智慧城市大量使用物联网技术存在安全风险；

（5）智慧城市关键技术存在失控风险。

具体建议如下：

（1）转变智慧城市安全建设思想，由同步建设转为安全先行；

（2）正确处理智慧城市与信息安全发展关系；

（3）确保智慧城市数据安全保护；

（4）制定物联网安全技术方向鼓励智慧城市关键技术引进和创新。

话题8：信创网络安全保障能力建设

信息技术创新应用作为我国信息技术领域打造自主创新生态的国家战略举措，也是新基建的重要抓手。未来3到5年，信创产品和解决方案将在更多领域规模化推广应用。其安全问题将面临前所未有的挑战，强化信创安全体系顶层设计、统筹构建安全保障体系。

话题9：区块链技术和产业创新发展

实现区块链技术规模化落地，需要突破跨链互通与协作、自主创新、标准规范建设方面、安全问题、监管机制和手段等方面问题。

具体建议如下：

（1）要加强标准规范建设，加快区块链关键急需标准和重点行业专用标准的研制，积极引导和支持主体参与区块链国际标准的研究、制定和推广；

（2）要加强关键技术攻关，推动区块链与5G、AI、大数据、物联网等其他新一代信息技术的创新融合，加快自主可控的区块链底层技术研发平台和基础设施平台建设；

（3）要加强产业政策供给，尽快出台区块链发展的顶层设计和总体规划，加强产业体系化布局；

（4）要加强监管体系建设，在坚决打击恶意违法行为的同时给新兴技术一定包容发展的空间，强化区块链平台级应用的安全评估，提升区块链技术及应用的合规性和规范性。

话题10：提高网络安全应急处置能力

具体建议如下：

（1）完善国家层面的网络安全应急管理制度体系；

（2）建设全国性网络安全应急管理处置平台；

（3）配套制定网络安全处置应急征用办法；

（4）研究开展必要的实战性网络安全测试。

人工智能、5G时代、物联网、网络安全等将如何影响我们生活?

(一) 人工智能：带人类进入前所未有的智慧社会

未来人类会慢慢习惯进入一个人工智能无处不在的社会，人工智能是时代进步的产物，它的发展让我们的生活越来越便利。人工智能方向很多，主要看具体场景如何落地。

目前人工智能和医疗结合应用超乎想象，尤其是在医学影像识别方面，早期筛查肿瘤的准确率已经超过普通医生的水平。人和机器可以互联互通，比如：预测人脑中可能会想什么，让瘫痪病人大脑里的信息传递给机器，通过大脑里的信息和指令直接让机器以比人类在智能手机上快 5 倍的输入速度打字。

揭露保险金融诈骗，保险行业是有利可图的诈骗目标。通过使用人工智能的，保险行业调查员可以发现以前隐藏的诈骗。人工智能帮助寻找失踪儿童，一个专门搜索失踪儿童的25人团队，每天收到大约22000条线索。通过使用人工智能来分析案例，该组织能够更快地将潜在线索提供给相应的权威机构。

人工智能被问及最多的一个问题是：未来人工智能会取代人类吗？阿里巴巴董事局主席马云说，人类对自己大脑的认识不到10%，10%创造出来的机器不可能超越人类，与其担心技术夺走就业，不如拥抱技术解决问题。

(二) 物联网：让世界万物连接在一起

什么是物联网？有人举了一个例子：在药片中放入传感器吃下去，我们可以看到机器人蠕虫进入到身体里面协助医生做手术。这些万物互联的东西会越来越多地融入我们生活。

美国计算机科学家、图灵奖获得者、“互联网之父”罗伯特·卡恩提出“数字物体”互联网系统的现有物联网的拓展。“互联网解决了人与电脑的连接问题，物联网将让世界万物连接在一起。”

“在这个智能互联网的时代，越来越多的设备都因具有计算、存储、网络等功能而变得更加智能。”在各种传感器的辅助下，这些智能终端可以不断地感知周围环境，从而在云端汇聚成几何级增长的海量数据。

在工作场景应用中，将出现能自动学习用户使用习惯的智能情境引擎，支持24种语言的服务机器人，混合现实智能眼镜等；在日常生活应用中，将产生智能心电衣、智能电视、智能音箱等。

(三) 5G时代：正在向我们走来

早晨醒来，智能家居已经为你煮好了早餐；出门时，你乘坐的是无人驾驶汽车——这仅是令人期待的5G时代的一个侧面，5G时代正向我们走来。我国三大通信运营商，已于2018年迈出5G商用第一步，工信部已于2019年6月6日正式发放5G牌照，从而使我国进入5G时代，并力争在2020年实现5G的大规模商用。

5G有三大应用场景：增强移动宽带，超可靠低时延，支撑移动互联网和产业互联网的发展。5G时代的信息传播将会是智能的、互联的、配备智能技术和传感器，支持人与人、人与物、物与物，以及环境之间的信息交互，这将带来更多用户端的创新应用。

对于中国的5G时代，以中兴、华为为代表的中国企业，已经走在5G时代的世界前列。面对即将到来的物联网时代，5G是被看做推动物联网发展的最好推手，但是物联网规模急剧扩大也将带来新的安全隐患。

（四）网络安全：推动打击网络犯罪国际合作

智能设备和可穿戴设备快速增多，在线内容爆炸式增长……互联网已经渗透到生产生活的方方面面。然而，数据泄露、网络诈骗、网络攻击频发，前沿技术应用带来的潜在安全风险受到关注，人工智能、物联网技术广泛应用更是不断引发担忧。

中国互联网协会研究中心秘书长吴沈括说，目前我国网络犯罪占犯罪总数近三分之一，每年以近30%幅度上升，已成为第一大犯罪类型。

据外交部提供的统计数据显示，我国所调查的网络犯罪案件中，很多违法网站和僵尸网络控制服务器位于外国特别是网络资源发达国家，不少犯罪行为通常使用跨国互联网企业提供的邮箱、即时通讯等网络服务。因此迫切需要推动打击网络犯罪国际合作，特别是制定相关的全球性法律文书，为各国共同打击网络犯罪提供法律基础。

随着5G时代，万物互联时代到来，新形势下的安全问题也日益严峻，我们在为新兴技术带来想象空间欢欣鼓舞的同时，也必须正视由此带来的安全挑战。一方面，要深入了解新型网络技术的安全需求；另一方面，要善用网络安全中的新型技术。两者相辅相成，相互促进，共同发展。

上网安全

1 如何防范病毒或木马的攻击

1. 为电脑安装杀毒软件，定期扫描系统、查杀病毒，及时更新病毒库、更新系统补丁。

2. 下载软件时尽量到官方网站或者大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒。

3. 不随意打开不明网页链接，尤其是不良网站的链接，陌生人通过QQ给自己传链接时，尽量不要打开。

4. 使用网络通信工具时不随意接收陌生人的文件，若接收可取消“隐藏已知文件类型扩展名”功能来查看文件类型。

5. 对公共磁盘空间加强权限管理，定期查杀病毒。

6. 打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建

立名为autorun.inf的文件夹（可防U盘病毒启动）。

7. 需要从互联网等公共网络上下载资料转入内网计算机时，用刻录光盘的方式实现转存。

8. 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。

9. 定期备份，当遇到病毒严重破坏后能迅速修复。

2 如何防范QQ、微博、微信等账号被盗

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. 在多人共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。

3 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。

4 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。

4. 安全标志：支付相关的网站一般网址以https开头，在网络地址栏会有彩色图标或锁头，可点击查看网站被权威机构认证的信息。

5. 悬停鼠标：不盲目相信搜索引擎的推荐，不乱点击邮件、微信、微博、短信中的网址，尤其是短网址。

5 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”。

6 如何防范假冒网站

假冒网站的主要表现形式有两种：一是假冒网站的网址与真网站网址较为接近；二是假冒网站的页面形式和内容与真网站较为相似。

1. 直接输入所要登录网站的网址，打开地址栏左侧的网站认证图标，观察内部信息判断网站是否合法，不通过其他链接进入。

2. 登录网站后留意核对所登录的网址与官方公布的网址是否相符。

3. 登录官方发布的相关网站辨识真伪。

4. 安装防护软件，及时更新系统补丁。

5. 当收到邮件、短信、电话等要求到指定的网页修改密码，或通知中奖并要求在领取奖金前先支付税金、邮费等时，务必提高警惕。

7 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。

8 如何防范网络诈骗

网络诈骗类型有如下四种：一是利用 QQ 盗号和网络游戏交易进行诈骗，冒充好友借钱；二是网络购物诈骗，收取定金骗钱；三是网上中奖诈骗，指犯罪分子利用传播软件随意向互联网 QQ 用户、MSN 用户、邮箱用户、网络游戏用户、淘宝用户等发布中奖信息；四是“网络钓鱼”诈骗，利用欺骗性的电子邮件和伪造的互联网站进行诈骗活动，获得受骗者财务信息进而窃取资金。

预防网络诈骗的措施如下：

1. 不贪便宜，仔细甄别，严加防范。

2. 使用比较安全的支付工具。

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先付款的信息，不要轻易把自己的银行卡借给他人。

5. 提高自我保护意识，注意妥善保管自己的私人信息，不向他人透露本人证件号码、账号、密码等，尽量避免在网吧等公共场所使用网上电子商务服务。

9 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。

10 如何保护网银安全

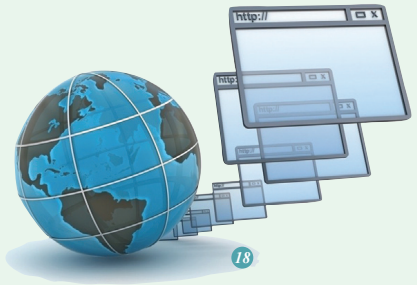
1. 尽量不在多人共用的计算机上使用网银，发现异常时及时修改密码并向银行求助。

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”，尽量使用软键盘输入账号及密码。

4. 交易完成后及时退出并拔下 U 盾。

5. 对网络单笔消费和转账进行金额限制，并开通短信提醒功能。



11 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。

12 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时，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。

13 如何防范网贷诈骗

1. 正规的贷款机构，在放款前是不会收取任何费用的；

2. 群众选择了贷款机构后，务必亲自到公司进行考察；

3. 不要轻信“无抵押贷款、当天放款”等广告标语，而且这项贷款仅凭身份证是不能办理的。并且，银行对无抵押贷款是有很严格要求的。因此群众在申请贷款的时候一定要谨慎，以免上当受骗。

4. 不要过分依赖网络，遇到有人借款，要牢记“不决断晚交钱，睡一觉过一天，再找亲人谈一谈”的口诀，多留一点时间给自己思考核实相关情况。

5. 一旦发觉对方可能是骗子，马上停止汇款，防止扩大损失。

6. 马上进行举报，可拨打官网客服电话、当地派出所电话或110报警电话，向有关部门进行求证或举报。

14 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关报案。

3. 配合公安机关或发卡银行做好调查、举证工作。

终端安全

1 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。

4. 运行安全扫描：安装安全软件，进行Wi-Fi环境等安全扫描，降低安全威胁。

2 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。

3 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短信，不向陌生帐号转账。

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。

4 如何防范病毒和木马对手机的攻击

1. 为手机安装安全防护软件，开启实时监控功能，并定期升级病毒库。

2. 警惕收到的陌生图片、文件和链接，不要轻易打开 QQ、微信、短信 、邮件中的链接。

3. 到权威网站下载手机应用。

5 如何防范骚扰电话、电话诈骗、垃圾短信

用户使用手机时遭遇的垃圾短信、骚扰电话、电信诈骗主要有以下四种形式：一是冒充国家机关工作人员实施诈骗；二是冒充电信等有关职能部门工作人员，以电信欠费、送话费等为由实施诈骗；三是冒充被害人亲属、朋友，编造生急病、发生车祸等意外急需用钱，从而实施诈骗；四是冒充银行工作人员，假称被害人银联卡在某地刷卡消费，诱使被害人转账实施诈骗。在使用手机时，防范骚扰电话、电话诈骗、垃圾短信的主要措施如下：

1. 克服“贪利”思想，不要轻信，谨防上当。

2. 不要轻易将自己或家人的身份、通讯信息等家庭、个人资料泄漏给他人，对涉及亲人和朋友求助、借钱等内容的短信和电话，要仔细核对。

3. 接到培训通知、以银行信用卡中心名义声称银行卡升级、招工、婚介类等信息时，要多做调查。

4. 不要轻信涉及加害、举报、反洗钱等内容的陌生短信或电话，既不要理睬，更不要为“消灾”，将钱款汇入犯罪分子指定的账户。

5. 对于广告“推销”特殊器材、违禁品的短信和电话，应不予理睬并及时清除，不要汇款购买。

6. 到银行自动取款机（ATM 机）存款遇到银行卡被堵、被吞等意外情况，应认真识别自动取款机“提示”的真伪，不要轻信，可拨打 95516 银联中心客服电话了解查问。

7. 遇见诈骗类电话或信息，应及时记下诈骗犯罪分子的电话号码、电子邮件地址、QQ 号及银行卡帐号，并记住犯罪分子的口音、语言特征和诈骗的手段和经过，及时到公安机关报案，积极配合公安机关开展侦查破案和追缴被骗款等工作。

6 如何防范智能手机信息泄露

1. 利用手机中的各种安全保护功能，为手机、SIM 卡设置密码并安装安全软件，减少手机中本地分享，对程序执行权限加以限制。

2. 谨慎下载应用，尽量从正规网站下载手机应用程序和升级包，对手机中的 Web 站点提高警惕。

3. 禁用 Wi-Fi 自动连接到网络功能，使用公共 Wi-Fi 有可能被盗用资料。

4. 下载软件或游戏时，应详细阅读授权内容，防止将木马带到手机中。

5. 经常为手机做数据同步备份。

6. 勿见码就刷。

7 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。

8 如何正确扫描二维码

1. 不扫以礼品为幌子型二维码。

2. 不扫利益诱惑型二维码。

3. 不扫陌生人求帮助型二维码。

4. 不扫拉粉求支持型二维码。

5. 保护付款二维码：付款二维码是自己向对方付款，对方只需快速扫描二维码，输入支付金额即可完成交易，不可随便轻易发送给别人。

不要轻易扫描来路不明的二维码，即便要扫码也要通过微信扫码这种高安全性能的软件。扫描二维码时要使用正规扫码软件，安装手机安全软件，不泄露重要个人信息，不打开扫码后出现的安全状况不明的网站。扫码需谨慎，不贪小便宜。

9 如何防范虚假公众号

1. 关注公众账号时，不仅要看账号的认证名称，还要查看认证机构。

2. 通过微信活动获取礼包的行为都具有一定的风险性。

3. 在向微信公众账号付款之前，最好先联系微信官方客服进行确认 。

桌面安全

1 电脑使用过程中面临哪些安全隐患

1. 使用易于猜中的密码。
2. 对敏感文件不加密（聊天文件、邮箱、论坛、网银等）。
3. 对定制木马病毒缺乏防护功能。
4. 对社交网站利用不当泄漏个人信息。

2 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。

3 如何防范U盘、移动硬盘泄密

外接存储设备也是信息存储介质，所存的信息很容易带有各种病毒，如果将带有病毒的外接存储介质接入电脑，很容易将病毒传播到电脑中。日常使用应：

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。

4 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. 定期清理浏览器中本地缓存、历史记录以及临时文件内容。

3. 利用病毒防护软件对所有下载资源及时进行恶意代码扫描。

5 计算机中毒有那些症状

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。

6 为什么不要打开来历不明的网页、电子邮件链接或附件

互联网上充斥着各种钓鱼网站、病毒、木马程序。不明来历的网页、电子邮件链接、附件中很可能隐藏着大量的病毒、木马。一旦打开，这些病毒、木马会自动进入电脑并隐藏在电脑中，会造成文件丢失损坏甚至导致系统瘫痪。

7 勒索软件的防范建议

1. 拒付赎金：支付赎金会助长攻击者的气焰，攻击者还会通过用户支付赎金速度对用户财务、数据价值等情况进行分析，可能从此被盯上。

2. 防毒杀毒：尽量到官方网站下载软件，安装正规杀毒软件，运行下载软件之前先进行病毒扫描。

3. 及时更新：关注操作系统安全公告，及时安装安全补丁，尽早堵住漏洞。

4. 封堵端口：关闭无用的计算机服务/端口，开启Windows防火墙，减少被攻击的“通道”。

5. 做好备份：使用光盘/移动硬盘等介质，对文档、邮件、数据库、源代码、图片、压缩文件等各种类型的数据资产定期进行备份，并脱机保存。

1 容易被忽视的个人信息有哪些

个人信息是指与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的数据。一般包括姓名、职业、职务、年龄、血型、婚姻状况、宗教信仰、学历、专业资格、工作经历、家庭地址、电话号码（手机用户的手机号码）、身份证号码、信用卡号码、指纹、病史、电子邮件、网上登录账号和密码等等。覆盖了自然人的心理、生理、智力，以及个体、社会、经济、文化、家庭等各方面。

个人信息可以分为个人一般信息和个人敏感信息。

个人一般信息是指正常公开的普通信息，例如姓名、性别、年龄、爱好等。

个人敏感信息是指一旦遭泄露或修改，会对标识的个体信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

2 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。

3 网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，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。

4 当公民发现网上有泄露个人身份、侵犯个人隐私的网络信息时该怎么办

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。

5 如何保障使用者身份合法、信息数据使用安全

利用数字证书对使用者的身份进行认证，这种认证形式比常规的用户密码形式认证更可靠。

利用数字证书对传输的信息数据进行加密，这样只有拥有相应密钥的人才能解密看到原信息数据。

法律法规知识

中华人民共和国网络安全法

目录

第一章　总则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条　国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条　国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条　国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条　国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条　网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条　建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条　网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条　国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条　任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章　网络安全支持与促进

第十五条　国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条　国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条　国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条　国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条　各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章　网络运行安全

第一节　一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条　网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条　网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条　网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事

侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条　网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条　国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条　网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节　关键信息基础设施的运行安全

第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条　按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条　除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条　关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条　关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条　关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条　关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条　国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章　网络信息安全

第四十条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条　国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

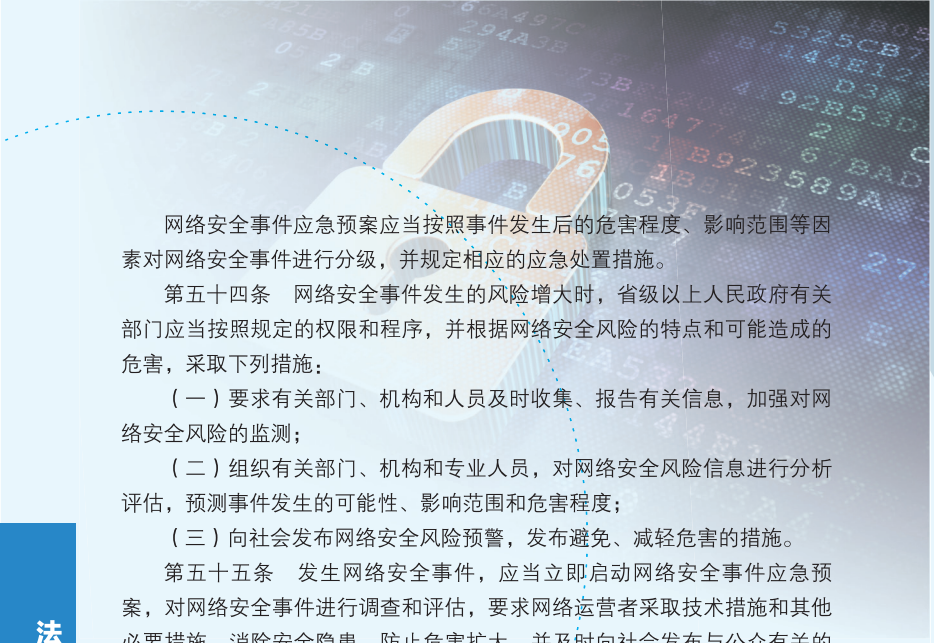
第五章　监测预警与应急处置

第五十一条　国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条　负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条　国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。



网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条　网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条　发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条　省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条　因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条　因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章　法律责任

第五十九条　网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条　违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条　网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条　违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条　违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十

万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条　网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条　关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条　关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条　违反本法第四十六条规定，设立用于实施违法犯罪活动的

网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条　网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条　网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条　发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条　国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条　网信部门和有关部门违反本法第三十条规定，将在履行网

络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条　违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条　境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章　附则

第七十六条　本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条　存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条　军事网络的安全保护，由中央军事委员会另行规定。

第七十九条　本法自2017年6月1日起施行。

1 《儿童个人信息网络保护规定》

第一条 为了保护儿童个人信息安全，促进儿童健康成长，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》等法律法规，制定本规定。

第二条 本规定所称儿童，是指不满十四周岁的未成年人。

第三条 在中华人民共和国境内通过网络从事收集、存储、使用、转移、披露儿童个人信息等活动，适用本规定。

第四条 任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。

第五条 儿童监护人应当正确履行监护职责，教育引导儿童增强个人信息保护意识和能力，保护儿童个人信息安全。

第六条 鼓励互联网行业组织指导推动网络运营者制定儿童个人信息保护的行业规范、行为准则等，加强行业自律，履行社会责任。

第七条 网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。

第八条 网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。

第九条 网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。

第十条 网络运营者征得同意时，应当同时提供拒绝选项，并明确告知以下事项：

（一）收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围；

（二）儿童个人信息存储的地点、期限和到期后的处理方式；

（三）儿童个人信息的安全保障措施；

（四）拒绝的后果；

（五）投诉、举报的渠道和方式；

（六）更正、删除儿童个人信息的途径和方法；

（七）其他应当告知的事项。

前款规定的告知事项发生实质性变化的，应当再次征得儿童监护人的同意。

第十一条 网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和双方的约定收集儿童个人信息。

第十二条 网络运营者存储儿童个人信息，不得超过实现其收集、使用目的所必需的期限。

第十三条 网络运营者应当采取加密等措施存储儿童个人信息，确保信息安全。

第十四条 网络运营者使用儿童个人信息，不得违反法律、行政法规的规定和双方约定的目的、范围。因业务需要，确需超出约定的目的、范围使用的，应当再次征得儿童监护人的同意。

第十五条 网络运营者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制儿童个人信息知悉范围。工作人员访问儿童个人信息的，应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。

第十六条 网络运营者委托第三方处理儿童个人信息的，应当对受委托方及委托行为等进行安全评估，签署委托协议，明确双方责任、处理事项、处

理期限、处理性质和目的等，委托行为不得超出授权范围。

前款规定的受委托方，应当履行以下义务：

（一）按照法律、行政法规的规定和网络运营者的要求处理儿童个人信息；

（二）协助网络运营者回应儿童监护人提出的申请；

（三）采取措施保障信息安全，并在发生儿童个人信息泄露安全事件时，及时向网络运营者反馈；

（四）委托关系解除时及时删除儿童个人信息；

（五）不得转委托；

（六）其他依法应当履行的儿童个人信息保护义务。

第十七条 网络运营者向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行安全评估。

第十八条 网络运营者不得披露儿童个人信息，但法律、行政法规规定应当披露或者根据与儿童监护人的约定可以披露的除外。

第十九条 儿童或者其监护人发现网络运营者收集、存储、使用、披露的儿童个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当及时采取措施予以更正。

第二十条 儿童或者其监护人要求网络运营者删除其收集、存储、使用、披露的儿童个人信息的，网络运营者应当及时采取措施予以删除，包括但不限于以下情形：

（一）网络运营者违反法律、行政法规的规定或者双方的约定收集、存储、使用、转移、披露儿童个人信息的；

（二）超出目的范围或者必要期限收集、存储、使用、转移、披露儿童个人信息的；

（三）儿童监护人撤回同意的；

（四）儿童或者其监护人通过注销等方式终止使用产品或者服务的。

第二十一条 网络运营者发现儿童个人信息发生或者可能发生泄露、毁损、丢失的，应当立即启动应急预案，采取补救措施；造成或者可能造成严重后果的，应当立即向有关主管部门报告，并将事件相关情况以邮件、信

函、电话、推送通知等方式告知受影响的儿童及其监护人，难以逐一告知的，应当采取合理、有效的方式发布相关警示信息。

第二十二条 网络运营者应当对网信部门和其他有关部门依法开展的监督检查予以配合。

第二十三条 网络运营者停止运营产品或者服务的，应当立即停止收集儿童个人信息的活动，删除其持有的儿童个人信息，并将停止运营的通知及时告知儿童监护人。

第二十四条 任何组织和个人发现有违反本规定行为的，可以向网信部门和其他有关部门举报。

网信部门和其他有关部门收到相关举报的，应当依据职责及时进行处理。

第二十五条 网络运营者落实儿童个人信息安全管理责任不到位，存在较大安全风险或者发生安全事件的，由网信部门依据职责进行约谈，网络运营者应当及时采取措施进行整改，消除隐患。

第二十六条 违反本规定的，由网信部门和其他有关部门依据职责，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》等相关法律法规规定处理；构成犯罪的，依法追究刑事责任。

第二十七条 违反本规定被追究法律责任的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第二十八条 通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，依照其他有关规定执行。

第二十九条 本规定自2019年10月1日起施行。

2 即时通讯工具（如微信、腾讯等）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《即时通讯工具公众信息服务发展管理暂行规定》，明确要求：

（一）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”。

（二）新闻单位、新闻网站开设的公众账号可以发布、转载时政类新闻，取得互联网新闻信息服务资质的非新闻单位开设的公众账号可以转载时政类新闻。其他公众账号未经批准不得发布、转载时政类新闻。

（三）即时通信工具服务使用者从事公众信息服务活动，应当遵守相关法律法规。对违反协议约定的即时通信工具服务使用者，即时通信工具服务提供者应当视情节采取警示、限制发布、暂停更新直至关闭账号等措施，并保存有关记录，履行向有关主管部门报告义务。

3 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。

4 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。

5 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。

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

（一）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。

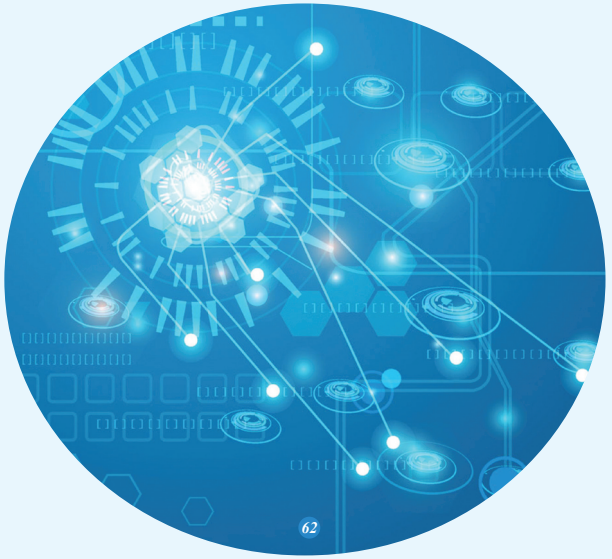
（二）将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的。

（三）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。

7 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。



8 移动互联网应用程序提供者应当依法履行哪些义务

2016 年 6 月 28 日，国家互联网信息办公室发布《移动互联网应用程序信息服务管理规定》，明确要求移动互联网应用程序提供者应当严格落实信息安全管理责任，依法履行以下义务：

（一）按照“后台实名、前台自愿”的原则，对注册用户进行基于移动电话号码等真实身份信息认证。

（二）建立健全用户信息安全保护机制，收集、使用用户个人信息应当遵循合法、正当、必要的原则，明示收集使用信息的目的、方式和范围，并经用户同意。

（三）建立健全信息内容审核管理机制，对发布违法违规信息内容的，视情采取警示、限制功能、暂停更新、关闭账号等处置措施，保存记录并向有关主管部门报告。

（四）依法保障用户在安装或使用过程中的知情权和选择权，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序。

（五）尊重和保护知识产权，不得制作、发布侵犯他人知识产权的应用程序。

（六）记录用户日志信息，并保存六十日。

安全笔记

网络安全为人民
网络安全靠人民

网络安全为人民
网络安全靠人民

2020年商洛市第七届
国家网络安全宣传周专题

主题日活动

9.15 校园日　　9.16 电信日　　9.17 法治日

9.18 金融日　　9.19 青少年日　　9.20 个人信息保护日