

网络安全宣传材料

2022年9月

①网络安全指导思想

习总书记重要讲话

2014年2月27日，中央网络安全和信息化领导小组第一次会议并发表重要讲话

网络安全已经上升为国家战略，成为国家安全的重要组成部分。习近平总书记指出：“**没有网络安全就没有国家安全**；网络安全和信息化是一体之两翼、驱动之双轮。必须统一谋划、统一部署、统一推进、统一实施；做好网络安全和信息化工作，要处理好安全和发展关系，做大协调一致、齐头并进，以安全保发展，以发展促安全，努力建久安之势，成长治之业。”

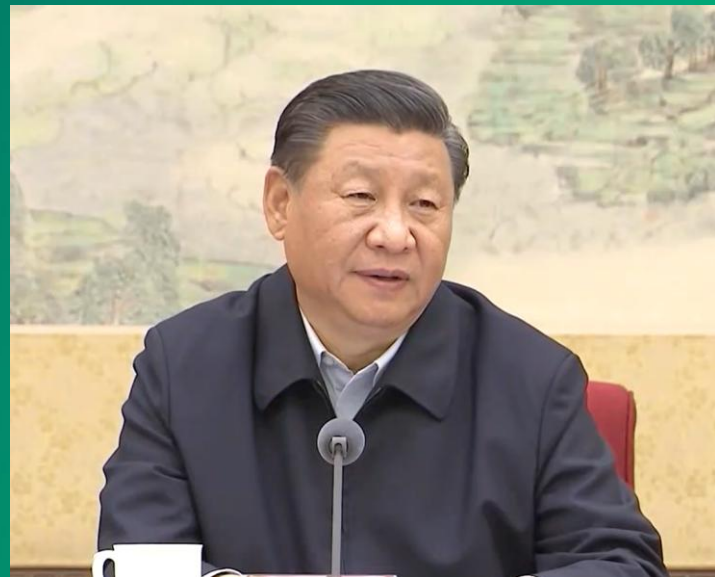


坚决打破“安全孤岛”

要提高公共安全体系精细化水平，从预判预警到应急处置，从现实生活到虚拟空间，每一个环节都要深入考虑和谋划。要构建公共安全人防、物防、技防网络，实现人员素质、设施保障、技术应用的整体协调，**彻底堵塞“安全漏洞”，坚决打破“安全孤岛”。**

——2015年5月29日

习近平总书记在十八届中央政治局第二十三次集体学习时的讲话



4.19重要讲话

“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上发表重要讲话，提出要**“坚持政策引导和依法管理并举”**，**“加快网络立法进程，完善依法监管措施，化解网络风险”**。习总书记的讲话为构建网络安全法律保障机制指明了方向，拓展了建设网络强国、提升网络空间国际治理能力的路径，是我国网络安全战略、顶层法律制度和具体规章制定的驱动力和催化剂。



在头脑中真正筑起网络安全的“防火墙”

这几年，全社会网络安全意识有了显著提高，但一些同志对网络安全认识还不到位，有的重发展轻安全、重建设轻防护；有的认为关起门来搞更安全，不愿立足开放环境搞安全；有的认为网络安全是中央的事、专业部门的事，同自己无关。这些看法都是不正确的。全党都要不断强化网络安全意识，在头脑中真正筑起网络安全的“防火墙”。

——2018年4月20日

习近平总书记在全国网络安全和信息化工作会议上的讲话



② 网络安全网络法规

网络安全发展史

1994年
《中华人民共和国计算机信息系统安全保护条例》

2008年《信息系统安全等级保护基本要求》
(GB/T22239-2008)

2017年9月
《公安机关信息安全等级保护检查工作规范(试行)》

2007年
《信息安全等级保护管理办法》

2017年6月1日
《中华人民共和国网络安全法》
开始实施

2019年12月1日
《信息安全技术—网络安全等级保护基本要求》
(GB/T 22239-2019) 实施

2020年1月1日《中华人民共和国密码法》
实施

2021年9月1日《关键信息基础设施安全保护条例》
实施

2021年9月1日
《中华人民共和国数据安全法》
实施

2021年11月1日
《中华人民共和国个人信息保护法》
实施

网络安全法



《中华人民共和国网络安全法》是为了保障网络安全，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，制定的法规。

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**；

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；

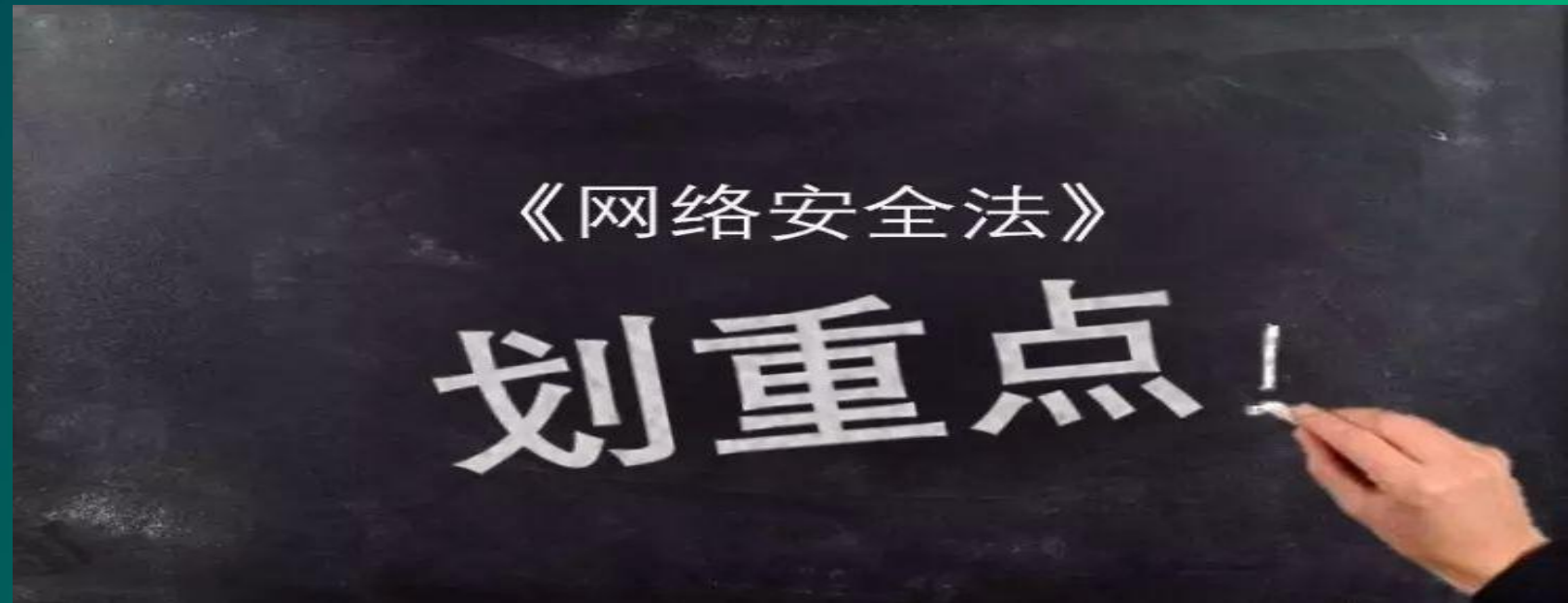
（四）制定网络安全事件应急预案，并**定期进行演练**；

（五）法律、行政法规规定的其他义务。

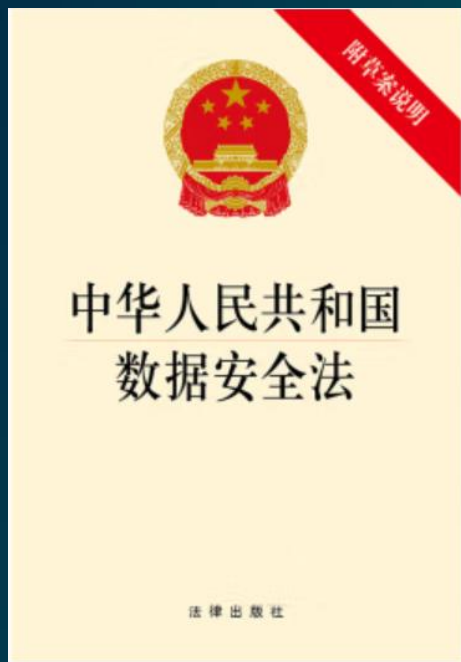
网络安全法

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。



数据安全法



《中华人民共和国数据安全法》2021年6月10日在中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行。数据安全法是我国第一部有关数据安全的专门法律，也是国家安全领域的一部重要法律。它的实施有助于进一步提升国家数据安全保障能力，应对因数据引发的国家安全风险与挑战。数据安全是指通过采取必要措施，保障数据得到有效保护和合法利用，并使数据持续处于安全状态的能力。

数据安全法

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并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可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上二十万元以下罚款。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、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十万元以上一百万元以下罚款。

个人信息保护法

2021年8月20日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》



作为中国首部针对个人信息保护的专门性立法，个人信息保护法将进一步强化个人信息安全监管与治理，把个人信息使用权关进法律的笼子里。

重要意义

- (1) 限制过度收集用户信息
- (2) 防止大数据“杀熟”
- (3) 加强保护个人敏感信息
- (4) 强化监管和违法惩戒

个人信息

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。

《网络安全法》

“公民个人信息”，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特定自然人身份或者反映特定自然人活动情况的各种信息，包括**姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹**等。

《中华人民共和国民法典》

“个人隐私”，是指自然人**基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动**等个人隐私和其他个人信息。

《最高人民法院、最高人民检察院-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》

个人信息保护法

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并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。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

(三)非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

③网络安全知识问答

Q&A



如何保护个人信息不被泄露？



- 1、培养安全意识，做到不主动透露个人信息，不被利益诱惑泄露个人信息；
- 2、养成安全习惯，如密码设置、软件及时更新、软件授权、数据备份、不随意连接WiFi、勿见二维码就刷等；
- 3、善用法律维权，当发现个人信息泄露的确凿证据时，积极向监管单位进行举报。



移动存储介质如何做好安全防护措施？



- 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。

Q&A



如何防止个人账号被盗?



账户和密码尽量不要相同，定期修改密码，增加密码的复杂度，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、密码尽量由大小写字母、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；

3、不同用途的应用账号，应该设置不同的用户名和密码；

4、在公共场所登录账号前重启机器，警惕输入账号密码时被人偷看；为防账号被侦听，可先输入部分账户名、部分密码，然后再输入剩下的账户名、密码；

5、涉及网络交易时，要注意通过电话与交易对象本人确认。

Q&A



如何安全地使用Wi-Fi?

1. 勿见到免费Wi-Fi 就用，要用可靠的Wi-Fi 接入点，关闭手机和平板电脑等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为不法分子设置的钓鱼陷阱，尤其是一些和公共场所内已开放的Wi-Fi 同名的信号。在公共场所使用陌生的无线网络时，尽量不要进行与资金有关的银行转账与支付

3. 修改无线路由器默认的管理员用户名和密码，将家中无线路由器的密码设置得复杂一些，并采用强密码，最好是字母和数字的组合



计算机中毒有哪些症状?



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

Q&A



如何辨别钓鱼邮件？



- 1、看发件人地址：如果是公务邮件，发件人多数会使用工作邮箱，如果发现对方使用的是个人邮箱帐号或者邮箱账号拼写很奇怪，那么就需要提高警惕。钓鱼邮件的发件人地址经常会进行伪造，比如伪造成本单位域名的邮箱账号或者系统管理员账号。
- 2、看发件的日期：公务邮件通常接收邮件的时间在工作时间内，如果收到邮件是非工作时间，需要提高警惕。比如，凌晨 3 点钟。
- 3、看正文目的：一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的，所以在收到邮件后要留意索要密码之类的要求，避免上当。
- 4、看正文内容：不要轻易点邮件中的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；有些垃圾邮件正文中的“退订”按钮可能是虚假的，点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码。
- 5、看附件内容：不要随意点击下载邮件中的附件，word、pdf、excel、PPT、rar 等文件都可能植入木马或间谍程序，尤其是附件中直接带有后缀为 .exe、.bat 的可执行文件，千万不要点击。

