网络安全培训

增强网络安全意识

北京环宇数通科技有限公司

C Directory

1

网络安全-基本概念

一 网络安全的基本概念

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

有句话讲什么是安全非常好：**客观上不存在威胁，主观上不存在恐惧。这是安全的最终目标。**

但是网络是由人员和信息系统组成的，事实上因为网络是飞速发展的，信息系统会越来越复杂。黑客组织犯罪日益猖獗，0day漏洞等不时爆出，人员的安全意识、操作也需要与时俱进，而且认知之外可能还有很多潜在安全威胁。

也就是说**没有绝对的安全。**

我们需要不断的提升信息系统的综合安全水平，来抵御可能到来的安全风险。

二 网络攻击的常见类型

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。有很多是商业信息，敏感信息，甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击（例如数据泄露、数据窃取、数据篡改、数据增删、木马病毒等）。

常见攻击类型

1.以可用性作为攻击目的，它毁坏系统资源，使计算机系统瘫痪不可用。（常见于商业竞争对手/国家攻防）

2.以保密性作为攻击目的，非授权用户通过某种手段获得对系统资源的访问，从而获得数据。（常见于黑客组织/商业对手/国家攻防）

3.以完整性作为攻击目的，非授权用户不仅获得访问而且对数据进行修改或者伪造。（常见于黑客组织）

三 网络安全的最终目的

通过采取必要的措施，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。

四 网络安全意识的培养

●为什么要培养网络安全意识？

1. **保护个人隐私：** 个人信息存储在互联网上，包括财务、身份证明、健康、住宿等。培养网络安全意识有助于保护个人隐私，防止敏感信息被不法分子滥用。
2. **防范网络犯罪：** 网络犯罪不断演变，涉及恶意软件、网络钓鱼等多种手段。提高网络安全意识，可以更好地识别和防范各类网络攻击。
3. **防止数据泄露：** 企业和个人存储大量敏感信息，包括商业机密、数据资产、研究成果等。通过培养网络安全意识，可以减少信息泄露的风险，维护商业和个人利益。
4. **遵守法规和法律：** 国家实施了许多网络安全法律法规，要求组织和个人采取措施来保护网络安全。培养网络安全意识有助于遵守法规，避免可能的法律责任。

●网络安全意识不足有哪些潜在危害？

相当一部分成功的网络攻击是从内部突破的，主要原因是人员安全意识不到位，可能的问题点例如：
1、可能会无意的造成数据泄露、木马携带。
2、操作和运维不规范、权限管理不规范、敏感文件和数据外发、u盘等便携式网络设备风险、弱口令、身份鉴别能力弱等。
3、网络设备不及时安装安全更新、打补丁和修复漏洞，甚至认为更新是没必要的，厌恶更新。

2 网络安全-风险和危害

一 网络攻击的主要手段有哪些

- 病毒、木马（常见威胁）
- 洪水攻击（常见威胁、难处理）
- 数据泄露（常见威胁）
- 社会工程学与欺诈（网络钓鱼、仿冒）
- 人为的特定攻击（APT）
- 无线与移动终端的安全威胁

网络安全的常见威胁

- 病毒、木马（常见威胁）

  常见载体

  —网页浏览

  —电子邮件

  —移动存储介质

  —即时聊天信息

  —网络下载

  —网络共享

NotPetya勒索病毒

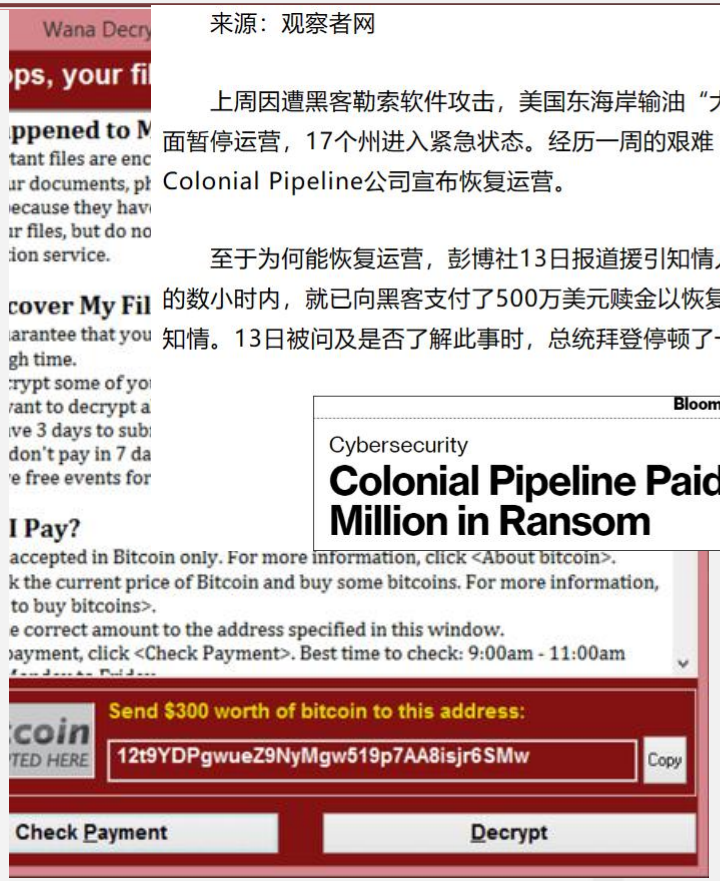
挂马暗链

挂马：主要特征是网页篡改，利用SQL注入、文件包含、跨站脚本等常见的网站漏洞获取权限，从而获得修改网页的能力。

暗链：应用开发者植入或者黑客入侵在源代码中植入的超链接，常见于政府gov.com、事业单位和教育edu.com等搜索引擎权重很高的网站中。利用其高搜索引擎权重，引导至博彩涩情等非法网站获利。

勒索病毒

勒索病毒已成为网络安全较大的威胁之一，勒索病毒入侵会对计算机系统数据进行加密勒索，导致数据泄露、数据丢失、企业业务中断等，从而带来严重的网络安全风险。尤其针对基础设施、企业用户的勒索，愈加猖獗。比较著名的有WannaCry（永恒之蓝）、NotPetya等，近年每年造成全球数百亿美元损失，并逐年递增。



来源：观察者网

上周因遭黑客勒索软件攻击，美国东海岸输油“大动脉”——运营商Colonial Pipeline公司被迫全面暂停运营，17个州进入紧急状态。经历一周的艰难“周旋”，终于在当地时间5月13日下午5点左右，Colonial Pipeline公司宣布恢复运营。

至于为何能恢复运营，彭博社13日报道援引知情人士的话称，其实Colonial公司早在勒索攻击发生的数小时内，就已向黑客支付了500万美元赎金以恢复系统。另有知情人士称，拜登政府官员对赎金一事知情。13日被问及是否了解此事时，总统拜登停顿了一下，然后说“对此无可奉告”。

Bloomberg

Cybersecurity

Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

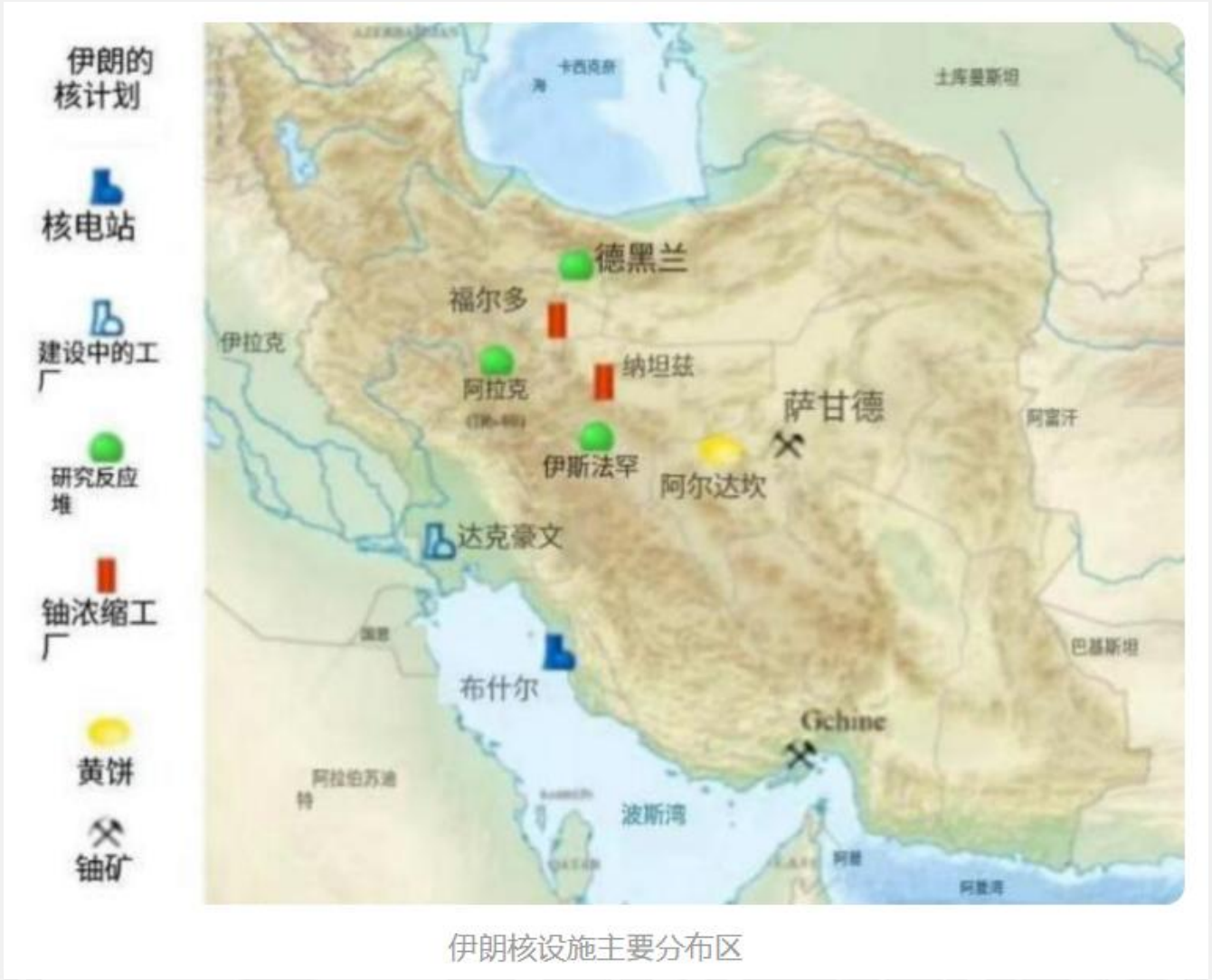
防范措施：规范网络行为；针对已知病毒及时更新操作系统以及业务软件、中间件等；勤打补丁、修复漏洞，使用先进的网络安全设备事半功倍；针对未知病毒做好备份工作，或者使用防勒索的安全产品。

震网病毒-首个精准攻击真实世界物理设施的网络战争

Stuxnet（震网病毒） 是一种计算机蠕虫病毒，大约写于 2005 年到 2010 年之间。最初攻击的目标是工业中的windows系统上的工控系统（PLC ），例如伊朗用的西门子PLC和winCC控制软件。

病毒特点：设计复杂精妙，极为善于隐蔽潜伏伪装，传播性强，发作不规律。可远程控制、信息篡改、数据窃取等，破坏力很强。

- 发起方：美国政府代号“奥运行动” 的APT组织
- 受害者：伊朗纳坦兹铀浓缩工厂；
- 攻击准备：长期情报搜集、规划准备和入侵潜伏作业；感染该工厂设备供应链承包商的内网并潜伏，通过U盘最终将病毒带入工厂机房，插入设备。
- 目的明确：阻断伊朗核武器进程为目的的攻击。
- 攻击过程：借助高度复杂的恶意代码和多个0day漏洞作为攻击武器；改变PLC工作频率，使离心机转数忽快忽慢，逐渐造成异常振动和应力畸变；
- 攻击结果：破坏了两千台离心机，并持续了8年



伊朗核设施主要分布区

三 网络安全中的数据泄露

●数据泄露

2023年数据泄露的平均成本达到了创纪录的445万美元，比2020年上涨了15%。泄露的数据一般有：

- 用户账号、密码
- 个人信息（身份证、住址、工作单位、电话号码、车牌、爱好、财产、行踪、通信、征信、医疗、生理健康、住宿等）
- 重要文件、企业经营活动等信息

这些信息多数时候都是有意或无意的情况下泄露出去的。

数据泄露事件一

2023年10月17日，LY（社交软件line） 关联公司的一名子承包商**员工电脑感染了恶意软件**，在访问公司系统时被攻击，泄露的内容包括：302569 条用户相关信息，86105 条合作伙伴相关信息、51353 条员工和其他人员相关信息。


LY

Lang

未授權存取造成資料外洩之公告與致歉

LY Corporation 察覺第三方曾未經授權存取公司系統（以下簡稱「此事件」），導致用戶、合作夥伴、職員、和其他人員*1 資料外洩。

我們希望以此公告讓用戶和相關單位掌握情況，我們也為可能造成的困擾和不便由衷致歉。

此外，如下文所述，我們已阻斷外部關係企業系統存取我們的任何伺服器，因為我們推測此次事件是經由此路徑存取我們的伺服器。至西元（下同）2023年11月27日為止，我們並未收到任何二次損害的舉報，包含用戶或合作夥伴資料之誤用，但我們仍將持續調查，隨時採取必要的應對措施。

北海某公司提供网上咨询服务，收集了个人和企业等大量公民信息，但未能按照《中华人民共和国数据安全法》《中华人民共和国网络安全法》以及有关等级保护工作要求落实网络安全保护主体责任。该网站服务器安全防护措施不足，被多个境外IP攻击入侵。涉案公司未采取数据加密等有效的技术保护措施来确保其收集的个人信息安全，**导致22万条个人信息泄露**；在发现个人信息泄露后，未及时告知用户，也未主动向公安机关履行报告义务；还存在网络日志留存不足6个月及相关安全管理制度缺失等问题。对此，北海公安机关对涉案公司及其直接负责人分别作出罚款20万元、3万元的行政处罚，并责令限期整改。

数据泄露事件二

万豪集团因数据泄露影响3.39亿客户，面临1.23亿美元罚款。

小米有品平台泄露个人隐私约2000万用户数据遭泄露。

华住旗下酒店用户注册信息、身份登记信息、开房信息大范围泄露，影响范围数亿。

黑客破解数据库，致物流公司78万条个人信息泄露。

顺丰快递3亿条信息疑似泄露，被挂网叫卖。

前程无忧51job泄露数百万条用户信息。

一百多家汽车厂商机密数据泄露，特斯拉通用大众丰田都中招。

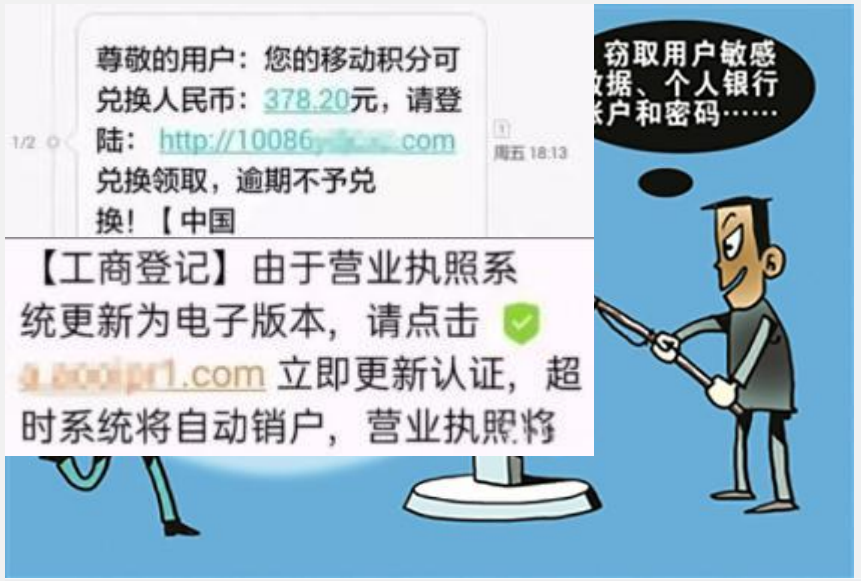
香港宽带公司一数据库被黑38万名客户信息恐泄露

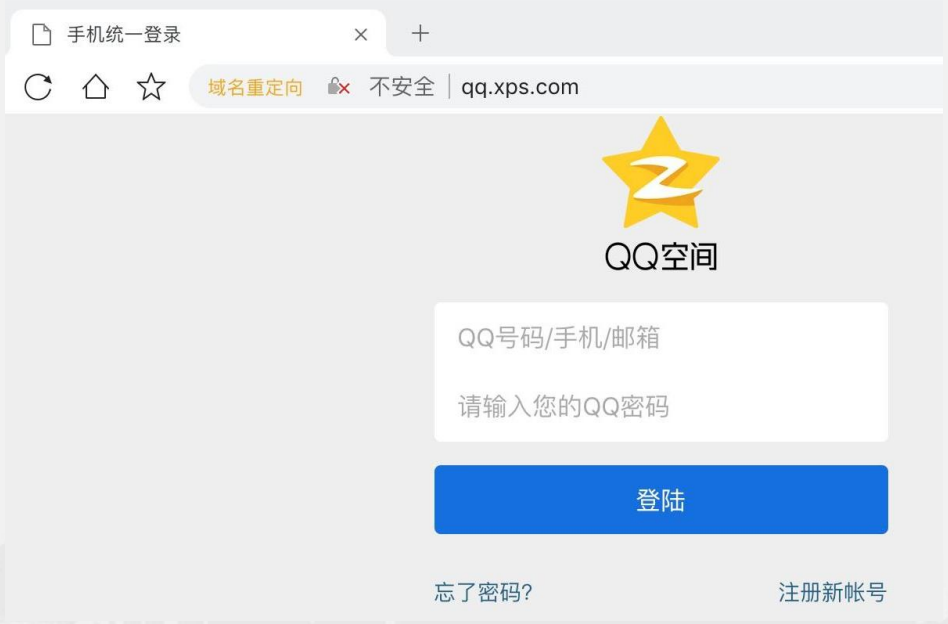
四 社会工程学与欺诈

- 社会工程学与欺诈

网页钓鱼、邮件欺诈、短信欺诈

- 网页钓鱼多数是仿冒网上银行或者有价值的网站引诱用户访问并盗取相关的账号及密码。
- 邮件欺诈包括：虚假的中奖信息、虚假销售信息、伪造管理员询问账号密码
- 短信欺诈多数是试图诱导用户进行银行转账、账户令牌授权等





五 人为的特定攻击（APT）

- APT（高级持续性威胁Advanced Persistent Threat）通过先进的攻击手段对特定目标进行长期持续性的网络攻击，一般针对大型企业及国家重要的基础设施和单位开展攻击。

- APT攻击的特点

1. 针对性强
2. 具有持续性
3. 隐蔽性强
4. 组织严密

六 无线和移动终端的安全威胁

- **无线设备和智能移动终端的风险：主要包含手机、路由器、随身WIFI、上网本、智能家居和其他物联网终端**

无线网络和数据传输：随意蹭网、使用未信任或者未加密的网络导致数据泄露、被监听等。

MAC地址欺骗：未使用强力的访问控制ACL和身份鉴别如802.1X，导致被MAC伪装欺骗。

伪基站或虚假信号广播：仔细鉴别发送的钓鱼短信、虚假广播信息等

信息泄露：恶意软件窃取信息、提权等。知名的有某多多安卓客户端恶意提权获取用户信息。

木马病毒：恶意软件会造成移动终端死机、运行慢、功能失效、重要文件被删除、数据泄露、被窃听等。

网络危害：恶意软件感染，强制移动终端不断发送垃圾信息(如骚扰电话、垃圾信息等)，或者成为僵尸网络的一员，被做成肉鸡执行DDOS攻击等行为。

七 为什么要培养网络安全意识

回到刚才的议题

为什么要培养网络安全意识？

- 培养良好的网络安全意识会让人员的网络行为习惯变得更加合理、安全，对单位、对个人是一种主动的保护。
- 平时在接触网络、使用网络时，要有意识的想想哪些行为会有安全风险。久而久之，会对一些网络风险有迅速的判断，变成基本常识。
- 可以有效保护企业数据安全、个人信息安全，极大程度避免被网络攻击成功，降低财产损失。
- 企业安全人员要多了解法律法规以及网络安全态势，帮助企业降低风险，包括应急演练、安全培训和维护企业安全制度等。
- 规避可能到来的法律风险。

接下来了解一下网络安全方面的法律法规。

3 网络安全-法律法规

2017年以来的网络安全相关法律和行政法规

发布时间	文件名称	发布机关	施行日期
2016年11月7日	《中华人民共和国网络安全法》	全国人大	2017年6月1日
2017年7月10日	关键信息基础设施安全保护条例	国家网信办	2021年9月1日
2018年6月28日	网络安全等级保护条例（征求意见稿）	公安部	
2017年6月27日	国家网络安全事件应急预案	中央网信办	
2017年5月19日	数据出境安全评估办法	国家网信办	2022年9月1日
2017年5月2日	网络产品和服务安全审查办法（试行）	国家网信办	2017年6月1日
2017年5月2日	互联网新闻信息服务管理规定	国家网信办	2017年6月1日
2017年5月2日	互联网信息内容管理行政执法程序规定	国家网信办	2017年6月1日
2017年6月1日	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	最高人民法院、最高人民检察院	2017年6月1日
2017年6月1日	网络关键设备和网络安全专用产品目录	国家网信办、工信部、公安部、国家认证认可监督管理委员会	2023年7月3日
2017年8月9日	公共互联网网络安全威胁检测与处置办法	工信部	2018年1月1日
2017年8月25日	互联网论坛社区服务管理规定	国家网信办	2017年10月1日
2017年8月25日	互联网跟帖评论服务管理规定	国家网信办	2017年10月1日
2017年9月7日	互联网群组信息服务管理规定	国家网信办	2017年10月8日
2017年9月7日	互联网用户公众账户信息服务管理规定	国家网信办	2017年10月8日

发布时间	文件名称	发布机关	施行日期
2017年10月30日	互联网新闻信息服务新技术新应用安全评估管理规定	国家网信办	2017年12月1日
2017年10月30日	互联网新闻信息服务单位内容管理从业人员管理办法	国家网信办	2017年12月1日
2017年11月23日	公共互联网网络安全突发事件应急预案	工信部	发布并施行
2018年2月2日	微博客信息服务管理规定	国家网信办	2018年3月20日
2018年6月19日	关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告	中国国家认证认可监督管理委员会	发布并施行
2018年6月27日	关于发布网络关键设备和网络安全专用产品安全认证实施规则的公告	中国国家认证认可监督管理委员会	发布并施行
2018年9月15日	公安机关互联网安全监督检查规定	公安部	2018年11月1日
2018年11月15日	具有舆论属性或社会动员能力的互联网信息服务安全评估规定	国家网信办	2018年11月30日
2018年12月26日	金融信息服务管理规定	国家网信办	2019年2月1日
2019年1月10日	区块链信息服务管理规定	国家网信办	2019年2月15日
2019年5月24日	网络安全审查办法	国家网信办	2020年6月1日
2019年5月28日	《中华人民共和国数据安全法》	全国人大	2021年9月1日
2019年5月31日	儿童个人信息网络保护规定	国家网信办	2019年10月1日
2019年7月2日	云计算服务安全评估办法	国家网信办、发改委、工信部及财政部	2019年9月1日
2019年7月22日	互联网信息服务严重失信主体信用信息管理办法（征求意见稿）	国家网信办	
2019年10月20日	《中华人民共和国个人信息保护法》	全国人大	2021年11月1日
2023年12月8日	网络安全事件报告管理办法（征求意见稿）	国家网信办	
2023年6月6日	人工智能法（草案）	纳入国务院立法计划	
2023年6月6日	网络数据安全管理条例	纳入国务院立法计划	

网络安全有哪些法律法规

网络安全的的法律法规

1994年2月18号发布的《中华人民共和国计算机信息系统安全保护条例》
1997年12月16号发布的《计算机信息网络国际联网安全保护管理办法》
1997年和2009年修订的《中华人民共和国刑法》
2016年11月7号发布的《中华人民共和国网络安全法》
2021年9月1日的《中华人民共和国数据安全法》
2021年11月1日的《中华人民共和国个人信息保护法》

《网络安全法》第五十九条 网络运营者不履行本法规定的网络安全保护义务的，由有关主管部门责令改正并给予警告、通报批评；拒不改正或者危害网络安全的，处一百万元以下罚款，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。

《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。

一 网络安全有哪些法律法规

网络安全的的法律法规

1994年2月18号发布的《中华人民共和国计算机信息系统安全保护条例》
1997年12月16号发布的《计算机信息网络国际联网安全保护管理办法》
1997年和2009年修订的《中华人民共和国刑法》
2016年11月7号发布的《中华人民共和国网络安全法》
2021年9月1日的《中华人民共和国数据安全法》
2021年11月1日的《中华人民共和国个人信息保护法》

《刑法》第二百八十六条 【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。

《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。

二 网络安全相关部门

我国网络与信息安全行业相关管理部门有：工信部（网络安全管理局）、网信办、公安部（网络安全保卫局）、市场监督管理局、国家保密局等及其下属地方单位。

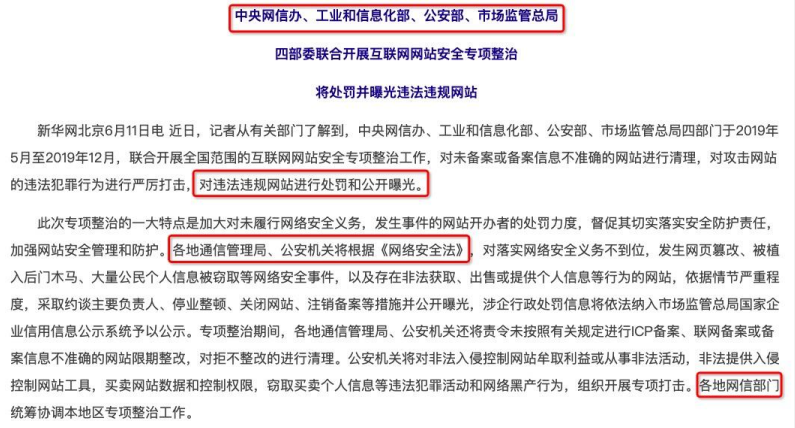
工信部负责组织拟订互联网及其相关网络与信息安全审查、规划、政策和标准并组织实施；指导督促电信企业和互联网企业落实网络与信息安全管理责任，组织开展网络环境和信息治理，配合处理网上有害信息，配合打击网络犯罪和防范网络失窃密；承担互联网网络与信息安全监测预警、威胁治理、信息通报和应急管理与处置；

中央网络安全和信息化委员会办公室：网信办负责监管互联网信息内容方面；打击和整治违法违规互联网信息传播现象（如整治涉恐、涉政、涉黑、涉暴、涉黄、涉毒等不良信息）；互联网舆情的监管以及引导；统筹协调网络安全工作和网络安全相关的监督管理工作。

公安部网安局：负责网络安全方面的监督和执法，比如负责全国信息安全等级保护制度的落实，网络治安维护，打击防范网络诈骗，网络黄赌毒等。开展网络安全宣传教育活动，普及网络安全知识。

三 国家级网络安全行动

国家监管力度不断增强，除了细化相关职能部门，出台相关法律法规，还会举行各种网络安全排查活动，打击网络犯罪，不断提升我国网络安全质量。



中央网信办、工业和信息化部、公安部、市场监管总局

四部委联合开展互联网网站安全专项整治

将处罚并曝光违法违规网站

新华网北京6月11日电 近日，记者从有关部门了解到，中央网信办、工业和信息化部、公安部、市场监管总局四部门于2019年5月至2019年12月，联合开展全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。

此次专项整治的一大特点是加大对未履行网络安全义务，发生事件的网站开办者的处罚力度，督促其切实落实安全防护责任，加强网站安全管理和防护。各地通信管理局、公安机关将根据《网络安全法》，对落实网络安全义务不到位，发生网页篡改、被植入后门木马、大量公民个人信息被窃取等网络安全事件，以及存在非法获取、出售或提供个人信息等行为的网站，依据情节严重程度，采取约谈主要负责人、停业整顿、关闭网站、注销备案等措施并公开曝光，涉企行政处罚信息将依法纳入市场监管总局国家企业信用信息公示系统予以公示。专项整治期间，各地通信管理局、公安机关还将责令未按照有关规定进行ICP备案、联网备案或备案信息不准确的网站限期整改，对拒不整改的进行清理。公安机关将对非法入侵控制网站牟取利益或从事非法活动，非法提供入侵控制网站工具，买卖网站数据和控制权限，窃取买卖个人信息等违法犯罪活动和网络黑产行为，组织开展专项打击。各地网信部门统筹协调本地区专项整治工作。

4 网络安全-行为守则

一 树立网络安全行为守则

网络安全行为守则：

- 网络安全行为守则是为了确保个人、组织或公司在使用网络设备时保持安全的一系列行为和规范。
- 网络安全行为守则是普遍适用的规定和建议，指导大家在工作生活中，养成安全、负责任的网络行为习惯，树立良好的安全认知。
- 正确的网络行为对个人、组织或企业都是一种保护。

基本理念：

- ✓ 增强法律法规意识：所有人都应了解并遵循与网络安全相关的法律和法规。
- ✓ 重视安全责任：网络安全人人有责，每个人都应该为自己的安全负责。
- ✓ 坚持持续改进：不断地对网络安全措施进行检查和完善，确保其始终有效。

二 践行网络安全行为守则

账密安全和多因素身份验证

1. **账密安全**： 使用国密（参考《中华人民共和国密码法》）密钥，或者使用强口令（普遍意义上的密码），定期更改口令，不共享账户信息，避免使用容易猜测的口令。密码字符包含：大写字母、小写字母、数字和英文特殊符号（'-!"#$%&()*,./:;?@[]^_`{|}~+<=>）。不要使用弱口令，例如123456、qwerty、love123等简单或者有意义的口令。

- 至少 12 个字符长，但 14 个或 14 个字符以上更好。
- 至少要使用三种以上的字符 组合。
- 不是可以在词典或人员、角色、产品或组织名称中找到的单词。
- 定期轮换密码，且与以前的密码明显不同。
- 自己容易记住，但其他人难以猜出。 如"1Tdhblk_Fcdhx2A"
- **最重要的一点**是不要把密码写在或者放在桌面、抽屉、笔记本等容易被看到的地方并注名是密码。

7 8 g * T W & 2 3 . Y 3 $
七八个星天外，两三点雨山前
(一条大河波浪宽，风吹稻花香两岸)

2. **多因素身份验证**：启用多因素身份验证提高账户安全级别，例如短信、人脸识别、指纹验证等。

多因素身份验证 (MFA) 是一种身份验证方法，要求用户除了密码以外至少再提供一个身份验证因素，或者至少提供两个非密码的身份验证因素，才能访问网站、应用或网络。不限于以下方式：

- 身份验证--特质卡片、U盘等介质
- 身份验证—强口令和PIN码
- 身份验证--生物识别：指纹，语音，虹膜扫描和其他物理特征
- 身份验证—短信、邮件
- 身份验证—手机令牌校验码
- 身份验证—网站专属APP扫描二维码

数据保护和隐私

- 1. **数据分级和加密**：企业需要做好数据分类，并根据数据敏感性、机密性、合规要求等方面的标准做好数据分级，完善数据全生命周期的管控，以及采用适当的加密技术保护数据存储的安全。
  - 建立数据访问权限：确保只有授权人员能够访问、修改或删除特定级别的数据。
  - 制定数据安全策略：为每个层级数据制定相应的安全策略。这包括加密、网络安全、设备管理等方面，以确保数据存储的安全性。
  - 监控和审计：建立监控和审计机制，以追踪对各个数据级别的访问和操作。
  - 审查和更新：定期审查数据分级标准和安全策略，以适应不断变化的业务环境和法规要求。
  - 应急响应：建立数据泄露应急响应机制，必须及时向网安部门和受损用户报告，采取补救措施降低危害。

- 2. **隐私保护**：在处理个人信息时要小心谨慎：尊重用户隐私，合法收集和处理个人信息；不要随意透露个人信息，如身份证号码、银行卡号、账号、密码等。
  - 根据《中华人民共和国个人信息保护法》等法律法规要求，规范企业在收集、存储、使用、加工、传输、提供、公开、删除个人信息时的行为。
  - 制定企业的隐私政策，明确数据收集和使用的目的，以及个人信息的保护措施并对用户公布，并确保隐私政策的透明度和易理解性。
  - 保护用户对其个人信息的掌控权，提供用户访问、更正、删除、注销个人信息的途径，并确保企业能够响应用户的请求。

网络设备和软件安全

- 1. **定期更新**:
  - 定期更新网络设备的固件和软件，以修复潜在的安全漏洞。
  - 及时更新操作系统、安装杀毒软件和打补丁等其他安全措施，确保系统免受已知漏洞的威胁。
- 2.**数据备份**
  - 数据备份是企业保护核心数据的重要手段，能有效降低勒索病毒、系统故障、自然灾害和运维事故导致的数据丢失和损坏问题。
  - 满足行业安全和合规要求。
  - 制定企业自身的RTO和RPO，并根据RTO和RPO，合理选择数据备份的方式、策略、备份地点。
- 3. **设备管理**:
  - 配置网络防火墙和入侵检测系统等安全设施，监控和阻止恶意网络流量。
  - 删除临时、过期等不再需要的账户和服务。
  - 限制员工安装未经批准的软件，防止恶意软件的潜在入侵，或者敏感数据外发。
  - 实施应用程序安全策略，包括代码审查和漏洞扫描，以确保软件的质量和安全性。

网络通信安全和恶意软件防范

- 1.**加密通信**：确保通信过程中的数据机密性和完整性。
  - 使用安全协议（如*SSL/TLS* 、 *IPsec* 、 *PGP* ）进行数据传输，防止数据被监听、泄露、篡改等；
  - 对未知的、采用不安全协议（http）或者使用不可信证书的网站，禁止访问；
- 2.**谨慎使用公共网络**：在使用公共网络（如咖啡店、图书馆等）时，要小心保护个人信息。避免在这些网络上执行敏感操作，如登录银行账户或输入信用卡信息。
  - 开放网络、WEP、WPA协议的wifi尽量不要使用，防止wifi钓鱼；
  - 最好使用WPA2/WPA3协议+AES加密的wifi。
  - 避免在这些网络上执行敏感操作，如登录银行账户或输入信用卡信息，防止中间人攻击；
- 3.**警惕恶意软件**：提高对钓鱼信息的警惕，不轻信来自未知来源或仿冒来源的信息和链接。
  - 仔细甄别短信、邮件、网页、链接、以及下载（校验哈希值等）等，避免被网络钓鱼或者被植入恶意软件。

5

网络安全-管理制度

一 安全管理制度

安全管理机制是指为了保障网络安全而制定的一系列管理策略、流程、制度和技术措施。其目的在于确保网络系统的机密性、完整性、可用性以及可追溯性。

- **制度目标**

整体安全目标： 保障企业资产和信息系统的完整性、可用性和机密性，以维护业务连续性和客户信任。

- **领导和组织架构**

领导责任： 企事业单位领导层对网络安全的责任，包括提供足够资源、支持和培训，确保安全意识贯穿整个组织。

安全团队： 设立专业的安全团队，负责制定、实施和监督安全政策和程序。

- **安全政策和规程**

安全政策： 制定清晰、全面的安全政策，明确员工在处理企业信息时的责任和义务。

规程和流程： 制定详细的安全规章和操作流程，确保员工按照标准操作，降低人为失误和漏洞的风险。

- **风险管理和评估**

风险评估： 定期进行企业内部和外部的风险评估，以识别和处理潜在的威胁和漏洞。

应急计划： 制定完备的应急计划，确保在面临安全事件时能够迅速响应和恢复业务。

- **数据安全管理体系**

数据分类分级：根据数据属性分类，根据敏感性、机密性和合规性等要求做好数据分级。

数据管理：全生命周期安全管控，保证数据存储和传输的安全，做好数据的备份。

一 安全管理制度

- **人员安全管理**

权限管理： 实施有效的权限细分管理，确保每位员工只能访问其工作职责所需的信息和系统。
员工培训： 提供定期的安全培训，或者派安全员参加专业的安全讲座，使员工了解最新的安全威胁和公司安全政策。

- **访问控制**

设备保护： 确保物理设备（服务器、网络设备等）存放在安全的环境中，限制物理访问权限。
访问控制： 实施有效的访问控制措施，包括门禁系统和身份验证，确保只有授权人员能够进入敏感区域。

- **技术安全措施**

网络安全： 部署强大的防火墙、入侵检测系统和反病毒软件，定期进行安全审查和漏洞扫描。
加密技术： 对敏感数据采用加密技术，并保障数据在传输和存储中的安全。

- **审计和监控**

安全审计： 定期进行安全审计，检查系统和员工的操作合规性，并采取纠正措施。
实时监控： 部署实时监控警报系统，及时发现并通知安全团队，应对潜在的安全威胁。

- **合规性**

法规遵从： 遵循适用的法规和法律要求，确保企业安全管理制度符合相关标准。

抵制不良网络信息　提升网络安全素养
增强自我保护意识　建立正确价值观念
遵守网络安全法规　营造清朗网络空间

鸣谢！