

网络安全意识培训



目

录

01

网络安全国内外形势

02

网络安全法律法规解读

03

网络暴力预防与日常安全

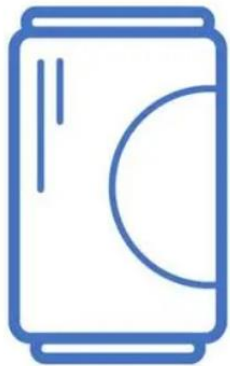


01

网络安全国内外形势

没有网络安全就没有国家安全

大数据应用无处不在



啤酒



纸尿裤

ORIGINAL



VARIATION



竞选网站

数据泄露的恶性事件频发

Facebook数据收集违规

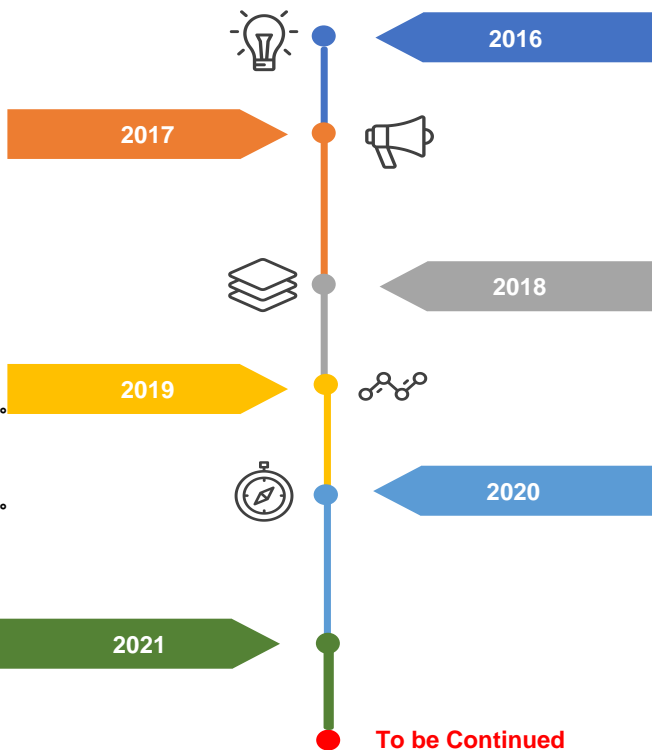
- Facebook因其数据收集涉及违规而遭到多国的罚款处罚。
- 违规原因在于未清晰告知用户信息收集的范围。

某人脸识别公司发生数据泄露事件

- 超过250万人的680万条记录泄露，其中包括个人姓名、身份证号码、性别、家庭住址和照片等。
- 据悉，此公司利用深度学习和人工智能等技术在监控视频中分析，用于人脸识别和人物画像分析。

阿根廷政府公民数据库疑全部泄露，攻击者待价而沽

- 攻击事件发生在9月，根据黑客提供的数据样本，他们已经掌握有阿根廷全体民众的全名、家庭住址、出生日期、性别信息、身份证签发与到期日期、劳工识别码、证照编号、公民编号以及身份证照片。



山东“徐玉玉案”

- 2016年“黑客”杜天禹通过技术手段非法入侵山东省高校招生平台，并窃取出售了64万余条考生信息。
- 这些信息被用作电信诈骗，获利14100余元。诈骗行为导致了徐玉玉的死亡。

支付宝数据收集违规

- 2018年初的“支付宝个人账单”采用默认同意的方式收集用户信息。
- 此举导致用户舆论不满，以及相关部门的约谈。

网络安全大事记

根据公开的泄露事件统计，2020年全球信息泄露用户凭证数达8.27亿个，泄露信息记录达352.79亿条，涉及人数约21.2亿人。

为了不上课，熊孩子能有多拼，你可能想象不到

2019年的逃课：

2020年的逃课：



据外媒报道，2020年一位来自佛罗里达州的 **16 岁高中生** 策划了 **八次 DDoS 攻击**，不仅让全校线上课程不得不终止了一段时间，还间接导致了地区级网络崩溃....

13小时前

这哥们干了我一直想干又不敢的事[捂脸]

回复

19

14小时前

这是人才啊！

回复 · 2条回复

8

16 岁少年如何黑掉学校网课平台的？

九月开学的第一天，当佛罗里达州迈阿密戴德县的私立学校南迈阿密高中的师生们打开虚拟教室，网络居然瘫痪了。

而这所学校的计算机网络是美国第四大计算机网络，校方考虑到开学第一天，当学生都登陆网课系统也有可能出现崩溃和网络卡顿的情况，但之后的几天里，这个网课平台却没有见好的气色，这让校方开始怀疑，可能有人动了手脚。

当地政府在联邦调查局、特勤局和佛罗里达州执法部门的协助下，追踪了迈阿密戴德学校的网络攻击，追踪到俄罗斯、乌克兰、中国、伊拉克和其他国家的 IP 地址，校方找到了这位“幕后凶手”。

并表示这是一次有预谋的恶意攻击，攻击者不是别人，正是学校里的一位 16 岁的在读学生。

“真凶”曝光！西北工业大学遭网络攻击



警情通报

2022年4月12日，西北工业大学向公安机关报案称，其邮件系统遭受境外黑客组织的网络攻击。我局迅速组织警力与网络安全技术专家成立联合专案组，对此案进行侦查。联合专案组克服重重困难，经过百余天艰苦攻关，案件侦查工作取得了重要进展，现简要通报如下：

经国家权威机构对从西北工业大学提取到的数据样本进行技术分析，结合联合专案组掌握的多种证据综合显示，此次西北工业大学遭受的网络攻击系具有美国政府背景机构及其雇员所为。相关机构和人员利用位于中国周边国家，已被其提前秘密远程控制的网络设备作为“跳板”，使用部署在美国本土的名为“酸狐狸”的中间人攻击平台及多种网络攻击武器对学校多个信息网络实施了大规模、持续性的网络攻击。

目前，我局已将有关情况通报西北工业大学并上报国家有关部门。下一步，我局将对该案继续开展侦查调查工作。

警方提示：网络安全关乎国家安全，关乎百姓切身利益，如遇有或遭受网络攻击行为，请及时向公安机关报案。

西安市公安局碑林分局

2022年9月5日 @西安碑林公安

2022年9月5日，国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告，调查发现，美国**国家安全局**

(NSA) 下属的特定入侵行动办公室（TAO）多年来对我国国内的网络目标实施了**上万次的恶意网络攻击**，控制了相关网络设备，疑似**窃取了高价值数据**

郑州一高校近万名学生个人信息遭泄露，责任人受处罚



致歉声明

日期：2020-06-10 编辑：

近日，我校在返校复学准备工作中发生了部分学生个人信息泄露事件，由此给学生和家长带来的不便，我们表示深深的歉意，向社会各界人士、广大网友、媒体的关心和批评表示诚恳的感谢。

我校在积极准备学生返校复学时，按照疫情防控要求，由教务科研处整理了计划返校学生名单，用以核查学生返校来源地及个人健康状况等信息。由于工作人员缺乏保密意识，造成部分学生的个人信息泄露，学校负有不可推卸的责任。

事件发生以来，我校在公安机关的帮助下查清了事情原委，及时成立三个工作专班，明确分工，专项排查，第一时间通知师生保护信息安全，不得随意转发，有效地控制了信息的进一步扩散。同时，我校对直接责任人予以解除劳动合同，对相关部门负责人及两名主管校领导予以记过处分，并将配合公安机关对其他涉嫌违法的行为严肃追究。

自1998年建校以来，郑州西亚斯学院虽然办出了一些特色，取得了一定成绩，赢得了学生、家长和社会的广泛信任，但在很多方面仍需继续提升。

我们深知，办学声誉和口碑来之不易、毁之易。通过这次事件，使我们意识到管理工作存在严重缺陷和不足，我们将尽最大努力弥补事件造成的损失，要求有关部门在全校范围内开展信息安全隐患排查。在今后的工作中，我们将深刻吸取教训，更加注重细节，坚决封堵漏洞，努力做到学生满意、家长放心、社会认可，不辜负社会各界对郑州西亚斯学院的信任和期望。

恳请广大师生、家长和社会各界人士继续监督、批评！

郑州西亚斯学院

2020年6月10日

- 2020年6月郑州某高校近两万学生个人信息被泄露，以表格的形式在微信、QQ等社交平台上流传。由于学校返校复学准备工作中发生了部分学生个人信息泄露事件，由此给学生和家长带来了不便
- 学校对直接责任人予以解除劳动合同，对相关部门负责人及**两名主管校领导予以记过处分**，并将配合公安机关对其他涉嫌违法的行为严肃追究。
- 公安局依据《中华人民共和国网络安全法》，对其负有领导责任的一名副校长和直接责任人进行了行政处罚

“滴滴”事件引发的数据安全思考

2021年6月30日，滴滴在美国纽约证券交易所上市。

没有敲钟，没有新闻通稿，没有铺天盖地的宣传。

什么都没有，一切静默得反常。

而滴滴上市的第二天，恰逢我党建党一百周年纪念日。

上市的重磅新闻，就隐藏在了党庆的消息中。

这还不是最蹊跷的。

更让人觉得离谱的地方在于：

2021年6月10号，也就是滴滴上市的20天前，我国刚刚公布了《中华人民共和国数据安全法》。

注意，我这里说的是北京时间。

而在美国纽约时间的6月10号，滴滴公司向美国证券委员会（SEC）递交了招股书，申请于纽交所上市。

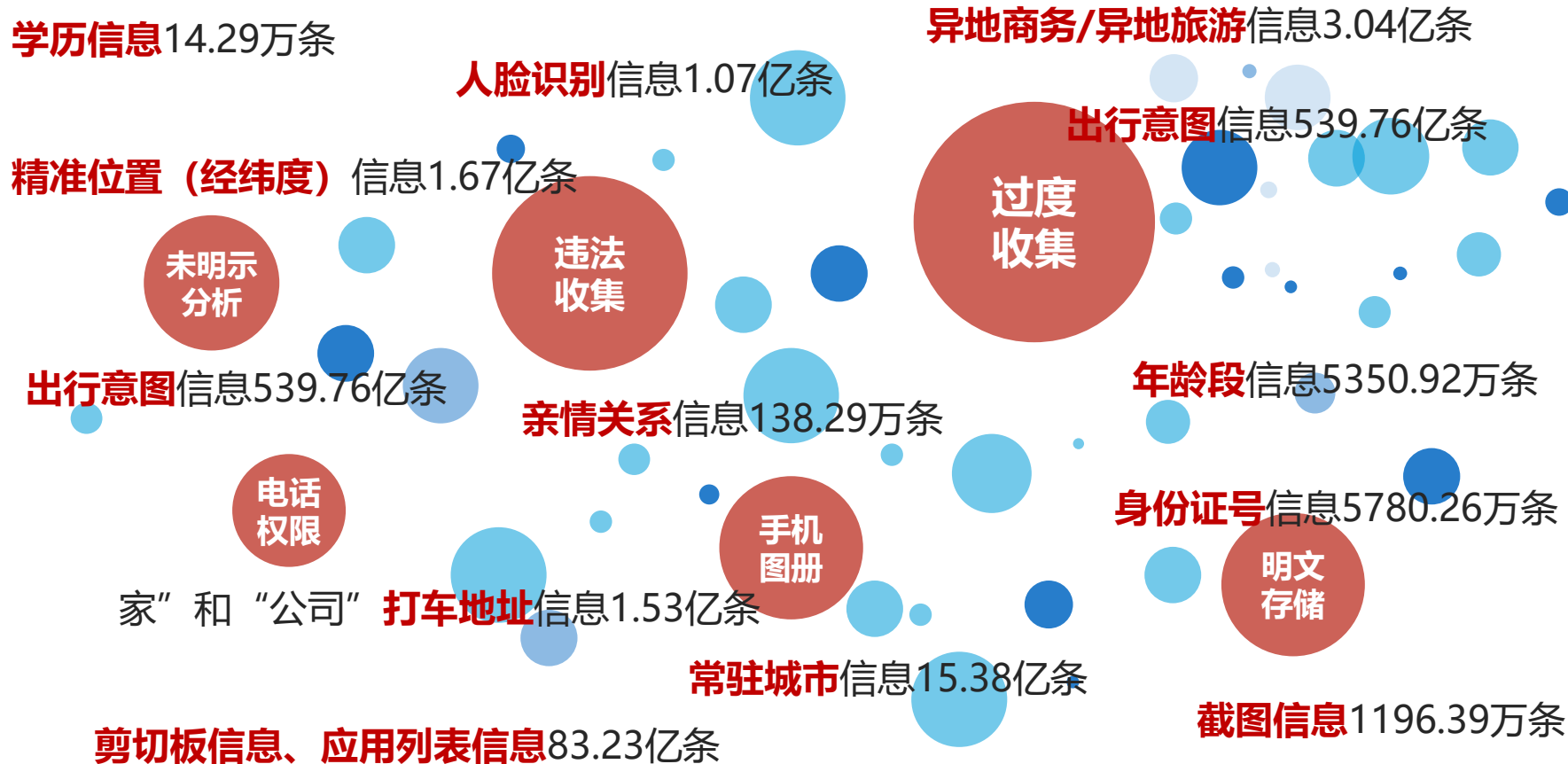
中美之间有12个小时的时差。

你可以简单地理解为：

白天国家颁布了《数据安全法》，晚上滴滴连夜向SEC纳了“投名状”招股书。



滴滴公司共存在16项违法事实，罚款80.26亿



公司市值蒸发超10亿，300万商铺遭瘫痪

关于微盟系统故障的通告

尊敬的微盟商户：

和您一样，我们一起度过了煎熬的 36 小时，我们预计此次故障还会持续一段时间，现就此次系统故障作如下通告：

2 月 23 日 19 点，我们收到系统监控报警，服务出现故障，随后我们立刻召集相关技术人员进行定位，发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。我们立刻启动紧急响应机制，并与腾讯云技术团队一起研究制定生产环境和数据修复方案。

截止到 2 月 25 日 7 点，我们的生产环境和数据修复都在有序的进行，我们预计 2 月 25 日晚上 24 点前我们的生产环境将修复完成，微盟所有新用户将可恢复服务，**老用户**由于数据修复时间问题，我们将提供临时过渡方案，我们预计老用户数据修复将可在 2 月 28 日晚上 24 点前完成。

@剧透娱乐圈

上海市宝山区人民法院刑事判决书（一审）（8 月 26 日宣判）摘录内容如下：

2020 年 2 月 23 日 18 时 56 分许，贺某酒后因生活不如意、无力偿还网贷等个人原因，在其暂住地上海市宝山区逸仙路 XXX 弄 XXX 号 XXX 室，通过电脑连接公司虚拟专用网络、登录公司服务器后执行删除任务，将微盟服务器内数据全部删除，导致微盟自 2020 年 2 月 23 日 19 时起瘫痪，300 余万用户（其中付费用户 7 万余户）无法正常使用该公司 SaaS 产品，经抢修于 3 月 3 日 9 时恢复运营（故障时间 8 天 14 个小时）。

截至 2020 年 4 月 30 日，造成微盟公司支付恢复数据服务费、商户赔付费及员工加班报酬等经济损失共计人民币 2260 余万元。

■ 那为什么一个普通运维人员有如此大能量？

- 很简单，不少互联网的运维人员基本都会有root权限，基本就是公司业务上帝级别的存在（`rm -rf /*`）
- 如果数据库操作权限分层分级，就很难出现这种情况！

个人信息泄露渠道



八大个人信息泄漏渠道

手机

5月13日，腾讯移动安全实验室发布今年一季度手机安全报告，统计发现近470万个软件包中，有读取用户隐私权限相关操作的软件比例达到71%。

报考

据报道，不少报考研究生的考生，在网上报名后连续收到内容为“提供考前绝密资料”的短信，大家一度怀疑自己的考试信息被学校泄露。

酒店

国内安全漏洞监测平台乌云近日发布报告，称如家、汉庭等大批酒店的开房记录被第三方存储，并且因为漏洞而泄露。

航空公司

近日，陆续有消费者通过微博投诉，称订购机票后个人信息遭泄露，涉及南航、东航、山东航空、深圳航空等多家国内知名航空公司。

网购

近日，“团委会团购网”的网页中出现了千余名会员的个人信息，内容包含会员名、电话号码及购买物品的内容等。

快递

近日，据央视报道，为了创收，圆通、申通、天天快递等快递公司会留存着单号等信息，价高就卖。

银行

余某为某银行职员，他将自己掌握的600余份客户信息出售，获利3万余元。这些个人信息被用作办理信用卡，并透支200余万。

保险公司

据央广报道，一家名为众宜风险管理机构的网站，可以随便在网站上查询客户投保信息，估计泄露的网页高达80万页。

网络安全事件层出不穷-国际



万豪酒店5亿客户数据泄漏



南美五国遭遇大停电，疑似美国网络攻击



东京奥运会遭遇黑客攻击



Facebook被爆泄露6亿用户密码



大数据公司Exactis泄露2.3亿个人隐私数据



AWS瘫痪：DNS被DDoS攻击15个小时

网络安全事件层出不穷-国内



超2亿中国求职者简历泄露
数据“裸奔”将近一周



华住旗下酒店信息泄露
涉及1.3亿人信息



台积电爆发大规模勒索病毒
损失达17.6亿元



拼多多现优惠券漏洞，遭黑产团伙盗
取数千万元

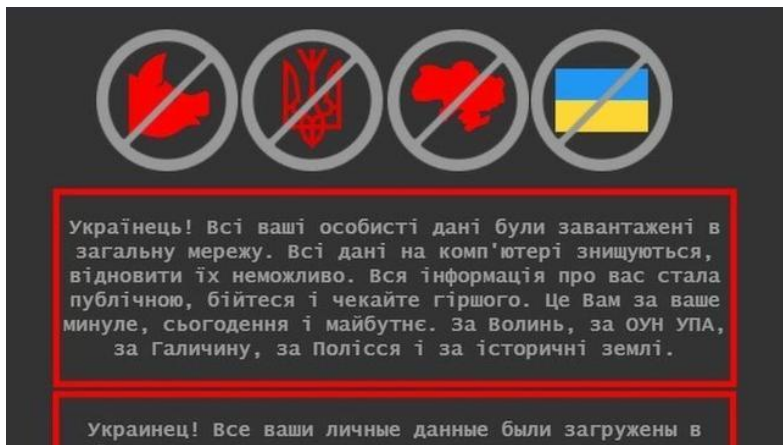
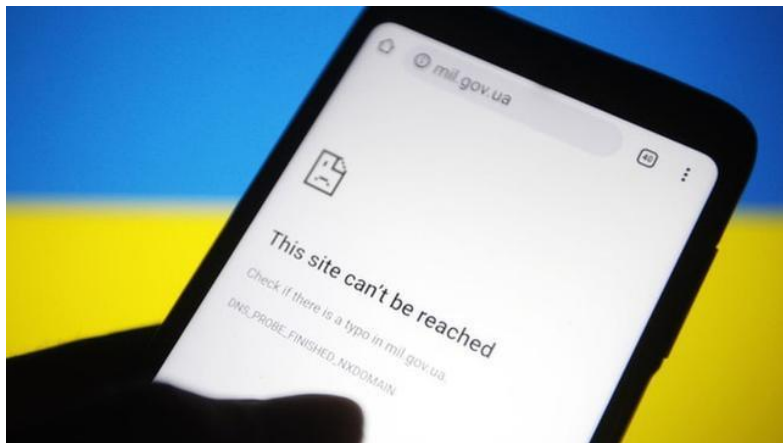


全国200多家三甲医院中招勒索病毒
医保系统中招勒索病毒
医院挂号系统中招勒索病毒



山东徐玉玉因被电信诈骗骗走9900
元学费，心脏骤停不幸离世

兵马未动 网络攻击先行



- 2022年2月24日，俄罗斯总统普京宣布对乌克兰展开军事行动。在此之前，乌克兰已经出现了频繁的网络遭受攻击的情况
- 2022年1月14日，乌克兰有大约70个政府部门的网站由于遭受DDoS攻击和黑客入侵而瘫痪。同时遭到攻击的还有Diia网站，这是一个包含政府服务的关键系统，存储有个人疫苗接种数据和证书。
- 从2月23日下午开始，乌克兰的政府、军事和银行网站开始遭受越来越严重的网络DDoS攻击，相继出现无法访问的状况
- 2022年2月24日，乌克兰国家紧急事务部门称，因为遭受网络攻击威胁，乌克兰已经切断互联网，全国境内无线和有线连接都将受限。

大数据时代，全球的数据博弈变得更加紧张

- 美国数据保护法律规定较为宽松，坚持以市场为主导、以行业自律为主要手段
- 加州作为先行者，第一个颁布数据泄露报告法，并在2018年通过了现行美国最严格数据隐私法案《加州消费者隐私法》
- 2019年美国司法部出台《云法案》

美国



欧盟



- 2012年，欧盟委员会提议GDPR取代1995年个人信息保护指令
- 2016年欧洲议会采纳GDPR草案，并正式发布法案
- 2018年GDPR正式实施

日本



- 2005年4月1日实施《个人信息保护法》，2015年进行大幅修正，2017年5月30日施行
- 2021年5月12日，日本国会通过了《为形成数字化社会完善相关法律的法案》，法案要求对个人信息保护制度进行审查修改，《个人信息保护法》修正案（以下简称“修正案”）作为完善法案一部分，也将与完善法案同时生效。

数据是已经成为新的生产要素，是国家基础性资源和战略性资源



国家高度重视网络安全、数据安全



02

网络安全法律法规解读

没有网络安全就没有国家安全

《网络安全法》政策全文



第一章	第二章	第三章	第四章	第五章	第六章	第七章
总 则	网络安全支持与促进	网络运行安全	网络信息安全	监测预警与应急处置	法律责任	附 则
14	6	19	11	8	17	4

《网络安全法》简介



《网络安全法》重要意义

第一点

制定《网络安全法》，
是维护国家网络空间主权、
安全和发展利益的重要举措。

第二点

制定《网络安全法》，
提高了社会的网络安全保护
意识和能力，明确了相关主
体的工作方向、义务和法律
责任。

第三点

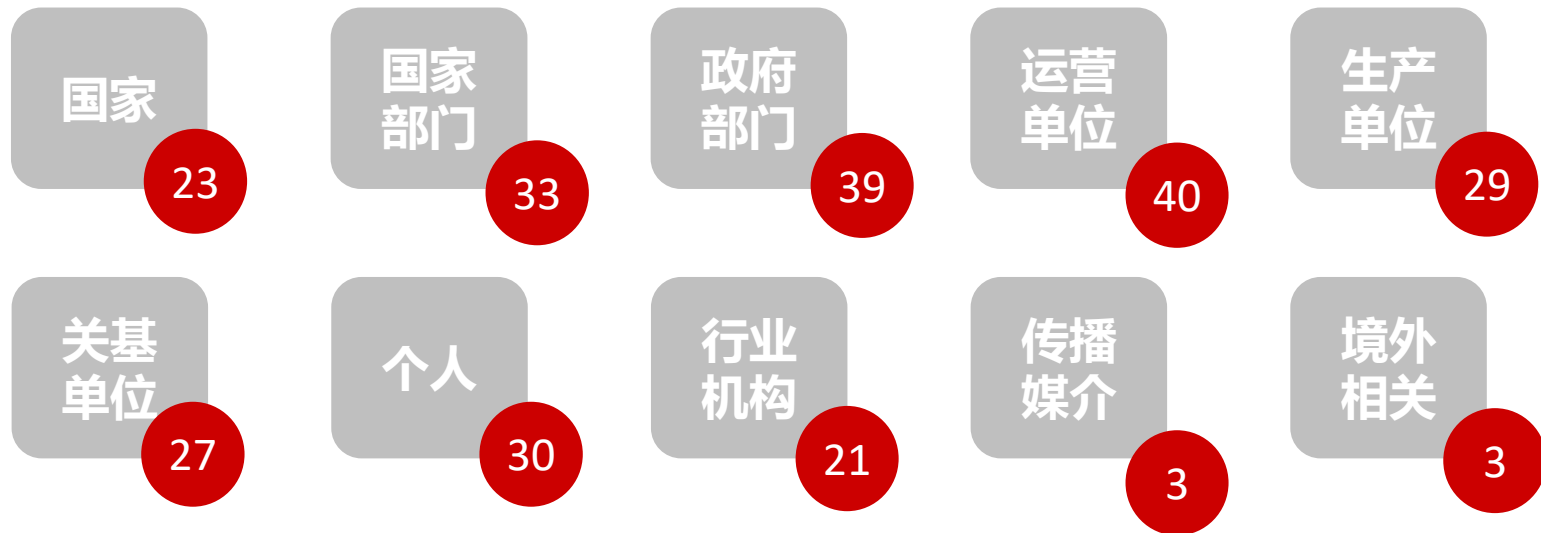
制定《网络安全法》，
是维护网络安全的客观需要，
为处理网络安全事件提供法
律依据。

第四点

制定《网络安全法》，
是参与互联网国际竞争和国
际治理的必然选择。

重点对象

重点对象



我国的网络安全基本制度

【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。

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。



个人和组织应尽义务

【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：

- (1) 不得危害网络安全
- (2) 不得利用网络从事危害国家安全、荣誉和利益
- (3) 煽动颠覆国家政权、推翻社会主义制度
- (4) 煽动分裂国家、破坏国家统一
- (5) 宣扬恐怖主义、极端主义
- (6) 宣扬民族仇恨、民族歧视
- (7) 传播暴力、淫秽色情信息
- (8) 编造、传播虚假信息扰乱经济秩序和社会秩序
- (9) 以及侵害他人名誉、隐私、知识产权和其他合法权益等活动

个人信息安全

【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。

网络安全教育培训

【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。

网络安全行业人才紧缺

年份 岗位	2021 年一季度		2022 年一季度	
	需求占比	平均薪资	需求占比	平均薪资
技术岗	64.6%	21182	67.6%	20235
销售岗	13.0%	14409	10.7%	15174
运营岗	4.9%	13872	4.0%	12599
职能岗	4.5%	7800	4.4%	8901
产品岗	4.2%	24347	4.7%	24706

2022年第一季度，网络安全领域的招聘比例进一步提升，其中技术人才招聘占比增至67.6%，平均招聘月薪为20235元

根据Compia公司最新发布的科技趋势报告，网络安全在2022年十大高薪紧缺技能中排名第一，TOP10榜单如下：

1. 网络安全
2. 云计算
3. 人工智能和机器学习
4. 数据分析和数据科学
5. 区块链
6. 开发运维
7. 增强现实/虚拟现实
8. 安卓/iOS开发
9. 用户体验/用户界面
10. 软件工程

目前每年高校安全专业培养人才**仅有3万余人**，今年各高校开设网络安全相关专业数据明显增加，但高校面临师资和设备短缺的问题尤为严重，学生在校**无法真正贴近实际环境进行有效地实践**，从而高水平技术型人才在各高校的实践能力养成方面存在较大差距

- 据中国网络安全产业联盟（CCIA）数据统计，2021年上半年，我国共有4525家公司开展网络安全业务，相比上一年增长27%。
- 值得关注的是，虽然2021年我国网络安全市场规模实现了20%以上的高速增长，但网络安全人才供给却并未保持同步增长。官方数据显示，**2021年，网络安全人才缺口达140万人**，预计2027年缺口将进一步扩大到**300万人**。网络安全工程师更是整个网络安全行业中的**极度稀缺人才**！

关注重点解读

对应法律责任

【第五十九条】（未履行网络运行安全义务的法律责任）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。

【第七十二条】（政务网络运营者不履行安全保护义务的法律责任）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。

三同步原则的重要性

【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。

两高司法解释

最高人民法院、最高人民检察院

【关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释】

此次出台的《解释》首次明确：如有网络平台泄露用户财产信息等**500条以上**、**通信信息5000条以上**、**伪造三个以上“钓鱼网站”**等违法情形，可按照刑法有关规定入罪，处以三年以下有期徒刑等。

处罚案例

处罚案例

2017年8月12日，蚌埠怀远县教师进修学校网站因网络安全防**等级保护制度落实不到位**，遭黑客攻击入侵。蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，**未落实网络安全等级保护制度，未履行网络安全保护义务**。

蚌埠市局网安支队依法对网络运营单位怀远县教师进修学校处以**一万五千元罚款**，对负有直接责任的副校长处以五千元罚款。安徽省公安厅网安总队**约谈分管副县长**。

- 执法机构：安徽省公安厅网安总队、蚌埠市公安局网安支队
- 处罚行为：未按规定履行网络安全等级测评义务
- 处罚措施：处罚、约谈
- 法律依据：《网络安全法》第21条、第56条、第59条第1款

处罚案例

处罚案例

2018年7月下旬，铜陵一网民金某因对公安机关处置某经济类案件不满，为了给公安机关施加压力，**多次在微信群中转发、传播不实信息和谣言，并积极煽动和组织其他网民参加非法集会**，造成了较为恶劣的社会影响。铜陵市公安局网安支队巡查发现该情况后，立刻对金某进行了调查取证并移交给属地公安机关依法处理。铜陵市铜官公安分局根据《网络安全法》第六十七条之规定，对金某处以**行政拘留十日**的处罚。

- 执法机构：铜陵市铜官公安分局
- 处罚行为：金某利用微信群转发、传播不实信息和谣言，煽动和组织他人参加非法集会
- 处罚措施：拘留十日
- 法律依据：《网络安全法》第46条、第67条

处罚案例

处罚案例

2018年9月28日，淮南市网络与信息安全信息通报中心接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在**高危漏洞**，**系统存储的4000余名学生身份信息已经造成泄露**。经查，确认淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，**未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施**，致使系统存储的4353名学生的身份信息泄露。10月12日，安徽省淮南市网警巡查执法官方微博发布通报称，淮南市公安局网安支队依法对该学院处以立即整改和行政警告的处罚措施。

- 执法机构：淮南市公安局网安支队
- 处罚行为：未按规定履行网络安全等级测评义务
- 处罚措施：责令整改，警告
- 法律依据：《网络安全法》第21条、第59条第1款

处罚案例

处罚案例

2020年1月，宿迁某科技公司经营的互联网数据中心未落实网络安全等级保护制度，存在未落实安全技术防护措施、未建立安全保护管理制度、未按规定保留网络日志等问题。同时，该公司还向部分未提供真实身份的客户，提供互联网接入服务。

宿迁警方依据《网络安全法》第21条、第24条及第59条、第61条规定，对该公司予以警告，责令限期整改。

- 执法机构：宿迁市公安局
- 处罚行为：未履行网络安全保护义务、用户身份管理义务案
- 处罚措施：责令整改，警告
- 法律依据：《网络安全法》第21条、第24条、第59条及第61条规定

处罚案例

处罚案例

2020年3月，接公安部通报线索，一款日语教学APP应用疑似存在侵害个人信息行为。经查，上海某教育科技有限公司常州分公司运营的一款日语教学APP应用，未向用户公开收集、使用个人信息规则，未明示收集使用信息的目的、方式和范围等。

常州警方依据《网络安全法》第41条、第64条规定，对该公司予以警告，责令限期整改。

- 执法机构：常州市公安局
- 处罚行为：未履行个人信息保护义务
- 处罚措施：责令整改，警告
- 法律依据：《网络安全法》第41条、第64条规定

处罚案例

处罚案例

2020年5月22日，当涂县公安局在侦办犯罪嫌疑人崔某（已起诉）侵犯公民个人信息案件中，发现违法嫌疑人张某在苏州市旧机动车交易市场鼎盛汽车贸易服务部上班期间，为获取二手车交易车辆抵押、保险等现实信息，从犯罪嫌疑人崔某处购买二手车交易当事人的**车辆信息共计164条，从事车辆买卖，从中非法获利**。

由于违法嫌疑人张某因合法经营购买公民个人信息数量及非法获利情况达不到刑事责任追责标准，但张某行为符合《网络安全法》第四十四条规定，其行为构成非法获取个人信息。当涂县公安局依据第六十四条第二款规定，决定对张某予以罚款**三万元处罚**。

- **执法机构：**马鞍山市公安局当涂县分局
- **处罚行为：**非法获取个人信息
- **处罚措施：**处罚、约谈
- **法律依据：**《网络安全法》第44条、第64条

对网络安全违法行为“0”容忍

汕头某公司未及时履行网络安全义务，网警依据网安法责令改正

2017-08-08 10:47:01 微信公众号“西交民巷23号”

腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》被立案调查

2017年08月11日 10:00:00

来源：中国网信网



【打印】 【纠错】

网信办约谈李文星事件涉事网站 责令BOSS直聘立即整改

重庆一网络公司未留存用户登录日志被网安查处

2017-08-01 22:13:22 来源: 中青在线(北京)

四川查处违反网络安全法首案：一网站因高危漏洞遭入侵被罚

2017-08-11 17:26:00 来源: 澎湃新闻(上海)

宿迁网警成功查处全省首例违反《网络安全法》接入违规网站案

株洲通报首起违反《网络安全法》案 一网络公司受行政处罚

14

2018-04-16 18:48

株洲新闻网

记者 李维熙

我要评论 0

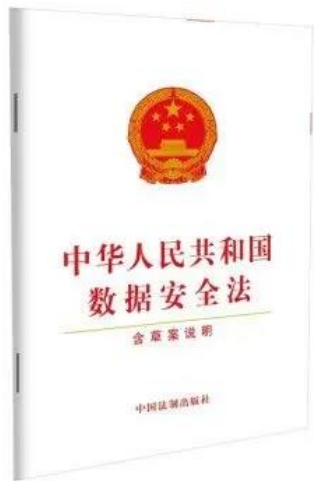
扫描二维码 分享

违规了！淘宝网等5家网站被责令限期整改

2017-08-17 19:04:34

来源：新华社

《中华人民共和国数据安全法》概要



第一章

总则

14

第二章

数据安全与发展

6

第三章

数据安全制度

19

第四章

数据安全保护义务

11

第五章

政务数据安全与开放

8

第六章

法律责任

17

第七章

附则

4

共7章55条5400余字 2021年9月1日起施行

《中华人民共和国数据安全法》概要

中华人民共和国数据安全法

- 数据安全法是总体国家安全观框架下，国家安全法律体系的重要组成部分。该法律在网络安全法的基础上，进一步明确了数据安全相关者的保护义务与职责，并与国家互联网信息办公室发布的《数据安全管理办法（征求意见稿）》相互照应。《数据安全法》的诞生，标志着数据安全上升到国家安全层面，意义重大。《数据安全法》共七章五十五条。

第一章 总则

主要规定了本法的立法目的、适用范围和工作原则，介绍了数据、数据处理及数据安全的定义，规定开展数据活动时必须遵守相关法律法规要求，不得危害国家、公共、社会及个人利益，违反者当依法进行处理。

第二章 数据安全与发展

主要介绍了数据开发与数据安全相辅相成的关系。数据安全发展路线，从实施大数据战略、加强技术的研究、标准体系建设、数据安全检测评估、认证的发展、到建立健全数据交易管理制度。同时，国家支持各类院校和企业等开展数据开发利用技术和数据安全相关教育和培训，促进人才交流。

第三章 数据安全制度

规定了数据安全主要管理制度内容，包括数据分类分级、数据安全风险评估、报告、信息共享、监测预警机制、数据安全应急处置机制、数据安全审查制度、数据出口管理制度。

第四章 数据安全保护义务

明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任，坚持安全与发展并重，规定支持促进数据安全与发展的措施。

第五章 政务数据开放与安全

规定国家机关应建立保障政务数据安全和推动政务数据开放的制度措施，大力推进政务数据资源开放和开发利用。

第六章 法律责任

规定了违反本法相关规定应当承担的响应法律后果。

第七章 附则

明确了涉密数据处理活动，统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动应当遵守有关法律、行政法规的规定，军事数据安全保护立法事宜以及本法的实施日期。

关注重点解读

总则

【第一条】为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

【第二条】在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

【第三条】本法所称数据，是指任何以电子或者其他方式对信息的记录。数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

【第六条】各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

关注重点解读

数据安全与发展

【第十四条】国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

【第十七条】国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

【第十八条】国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

【第十九条】国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

【第二十条】国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

数据安全制度

【第十四条】国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

国家数据安全协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

数据安全制度

【第二十二条】国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

【第二十三条】国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

【第二十四条】国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定。

【第二十五条】国家对于维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

数据安全保护义务

【第二十七条】开展数据处理活动应当依照法律、法规的规定，**建立健全全流程数据安全管理制度**，**组织开展数据安全教育培训**，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，**履行上述数据安全保护义务**。

重要数据的处理者应当明确数据安全负责人和管理机构，**落实数据安全保护责任**。

【第三十条】**重要数据的处理者**应当按照规定对其数据处理活动**定期开展风险评估**，并向有关主管部门**报送风险评估报告**。

风险评估报告应当包括处理的**重要数据的种类、数量**，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

关注重点解读

数据安全保护义务

【第三十一条】**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**重要数据的出境安全管理**，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的**重要数据的出境安全管理**办法，由国家网信部门会同国务院有关部门制定。

重要数据的处理者应当**明确数据安全负责人和管理机构**，**落实数据安全保护责任**。

【第三十六条】中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。**非经中华人民共和国主管机关批准**，境内的组织、个人不得向外国司法或者执法机构**提供存储于中华人民共和国境内的数据**。

关注重点解读

政务数据安全与开放

【第三十七条】国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

【第三十九条】国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

【第四十条】国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

【第四十一条】国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

关注重点解读

对应法律责任

【第四十四条】有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

【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。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

关注重点解读

对应法律责任

【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。

【第四十九条】国家机关不履行本法规定的数据安全保护义务的，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。

【第五十条】履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

【第五十一条】窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

个人信息泄露事件：海量人脸信息泄露、大数据杀熟

3·15晚会曝光 | 科勒卫浴、宝马、MaxMara商店安装人脸识别摄像头，海量人脸信息已被搜集！

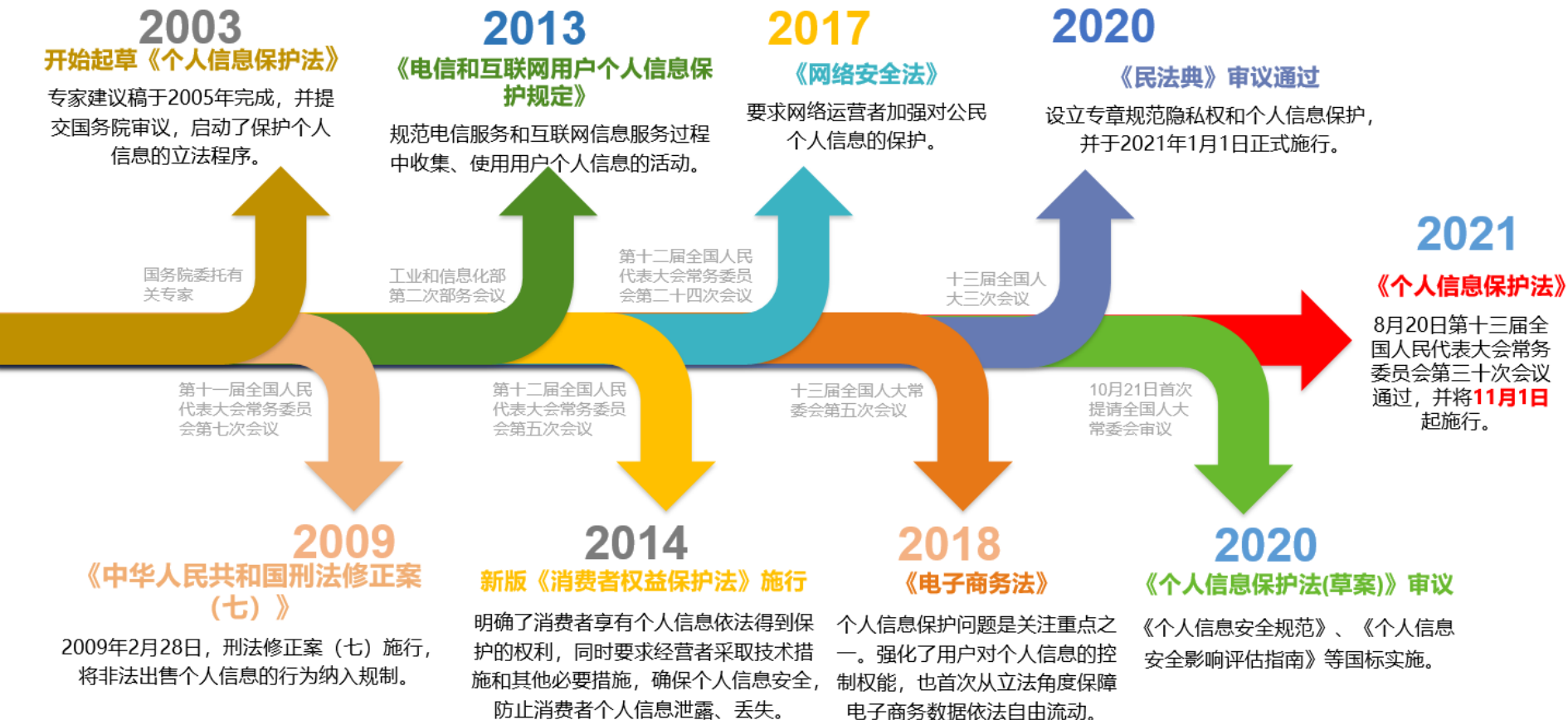
来源：央视财经 | 2021年03月15日 21:11

原标题：3·15晚会曝光 | 科勒卫浴、宝马、MaxMara商店安装人脸识别摄像头，海量人脸信息已被搜集！

商家在顾客们毫不知情的情况下，涉及顾客隐私、财产安全的人脸识别信息，被偷偷获取！



个人信息保护的“前世今生”



个人信息保护要点

关于履行个人信息保护职责的部门

- 明确国家网信部门负责个人信息保护工作的统筹协调，发挥其统筹协调作用；
- 同时规定：国家网信部门和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。

明确个人信息处理活动中个人的权利和处理者义务

- 一是，与民法典的有关规定相衔接，明确在个人信息处理活动中个人的各项权利；
- 二是，明确个人信息处理者的合规管理和保障个人信息安全等义务。

明确本法适用范围

- 一是，对本法相关用语作出界定；
- 二是，明确在我国境内处理个人信息的活动适用本法的同时，借鉴有关国家和地区的做法，赋予本法必要的域外适用效力，以充分保护我国境内个人的权益。

健全个人信息处理规则

- 一是，确立个人信息处理应遵循的原则；
- 二是，确立以“告知—同意”为核心的个人信息处理一系列规则等。

完善个人信息跨境提供规则

- 对跨境提供个人信息的“告知—同意”作出更严格的要求，同时对以下几类分别提出了管控要求：
- 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的处理者；
 - 因国际司法协助或者行政执法协助的；
 - 从事损害我国公民个人信息权益等活动的境外组织、个人等。



关注重点解读

总则

【第一条】为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，制定本法。

【第二条】自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

【第五条】处理个人信息应当采用合法、正当的方式，遵循诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

【第六条】处理个人信息应当具有明确、合理的目的，并应当限于实现处理目的所必要的最小范围、采取对个人权益影响最小的方式，不得进行与处理目的无关的个人信息处理。

【第七条】处理个人信息应当遵循公开、透明的原则，公开个人信息处理规则，明示处理的目的、方式和范围。

个人信息处理规则

【第十三条】符合下列情形之一的,个人信息处理者方可处理个人信息:

- (一) 取得个人的同意;
- (二) 为订立或者履行个人作为一方当事人的合同所必需;
- (三) 为履行法定职责或者法定义务所必需;
- (四) 为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;
- (五) 依照本法规定在合理的范围内处理已公开的个人信息;
- (六) 为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息;
- (七) 法律、行政法规规定的其他情形。

本法其他有关条款规定处理个人信息应当取得个人同意,但有前款第二项至第七项规定情形的,不需取得个人同意。

关注重点解读



池子池子大池子

今天 15:39

大家好我是池子。

我很久没说这句开场白了，很久没登台了，很多人问我，也不知道怎么说，我不喜欢散布负能量，但总得给个解释。这么多字我尽量有趣，实在不行你就当我是当街学驴叫。

大概情况是，去年我发现笑果文化违约，拖欠了很多应付的演艺报酬，而且没有按照合同给我账单明细，我提出异议之后 ... [展开全文](#)



2020年5月，脱口秀演员王越池（艺名“池子”）曾发布声明，称XX银行股份有限公司**泄露其个人账户信息**。XX银行随后发布致歉信称，王越池所反映一事属实，目前银行已按制度规定对**相关员工予以处分**，并对**支行行长予以撤职**。

2021年3月19日，此案件调查结果出炉，银保监会发布的行政处罚信息公开表显示XX银行的主要违法违规事实均指向客户信息收集、保护等方面，**被罚450万元**。



个人信息处理规则

【第十四条】处理个人信息的同意,应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的,从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的,应当重新取得个人同意。

【第十五条】个人信息处理者处理不满十四周岁未成年人个人信息的,应当取得未成年人的父母或者其他监护人的同意。

【第十六条】基于个人同意而进行的个人信息处理活动,个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

【第十七条】个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由,拒绝提供产品或者服务;处理个人信息属于提供产品或者服务所必需的除外。

个人信息处理规则

【第二十六条】个人信息处理者**不得公开其处理的个人信息**，取得个人单独同意的除外。

【第二十七条】在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的，不得公开或者向他人提供，取得个人单独同意的除外。

【敏感个人信息的处理规则】

【第二十九条】个人信息处理者具有特定的目的和充分的必要性，方可处理敏感个人信息。敏感个人信息是一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括**种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪**等信息。

个人信息处理规则

【第六十五条】违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，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；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、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**。

【第六十六条】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。

关注重点解读

个人信息处理规则

【第六十七条】国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门**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**。

【第六十八条】个人信息权益因个人信息处理活动受到侵害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

【第七十条】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**。

GB/T 35273-2020 个人信息安全规范

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据(通常称为元数据)等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码(如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等)等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

个人敏感信息判定

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14岁以下(含)儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用(如变更处理目的、扩大处理范围等)，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表B.1给出了个人敏感信息举例。

表B.1 个人敏感信息举例

个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

03

网络暴力预防与日常安全

没有网络安全就没有国家安全

你以为的玩笑其实已经成为网络暴力

- 我们常说“当心被雷劈”，虽是一句玩笑话，可有人真的遭遇了这种不幸。一对新人本来开心地拍着婚纱照，却突遇天降大雷，新郎被劈身亡。事件发生后，立刻登上了热搜。
- 这无疑是一起惨痛的悲剧。可评论区却出现了自以为幽默的抖机灵和无情冷血的嘲笑。

：下雨打雷天都要避一下，这点儿道理他都不懂吗？

25日

铁粉1:历劫失败🙏🙏🙏

22-8-26

:难道是发了什么毒誓天打雷劈之类。。

25

.这男的肯定上辈子没做好事

22-8-26

恶作剧引发的悲惨事件



13岁的梅根是提娜的女儿：**她很脆弱**，身体有点**超重**，**情绪**一直不太好。提娜说，上三年级时，梅根就开始讨厌自己，开始谈到**自杀**的话题，经常**沮丧**及**注意力不集中**



梅根曾央求了几个月的时间，最后母亲才同意她在MySpace上申请了一个帐户

梅根在网上结识了一个叫乔希 (Josh) 的16岁英俊男孩，乔希说她很漂亮

六周之后，乔希突然变脸，说她卑鄙，朋友们都觉得她很肮脏

遭到了巨大的侮辱后，梅根完全绝望了.....

网络暴力事件频发

虐猫事件

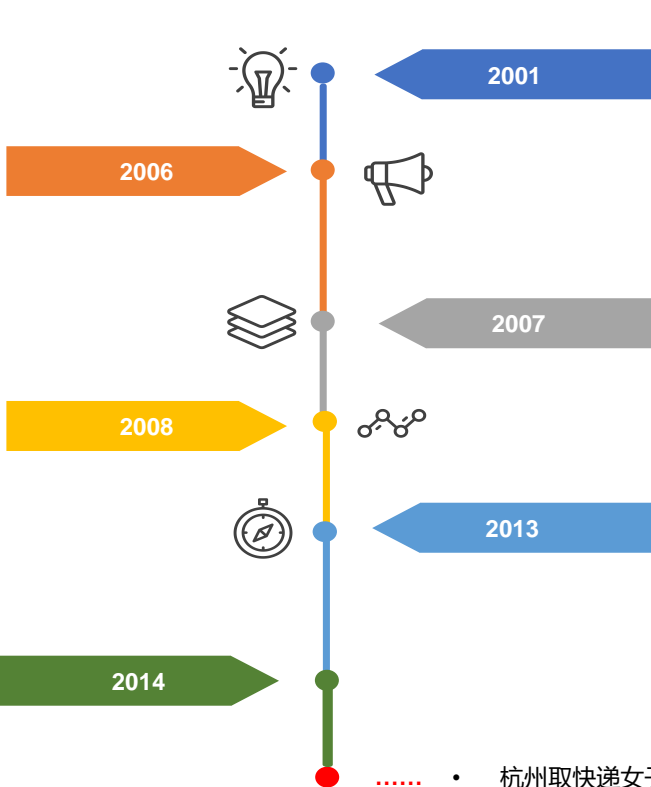
- 一网友公布了一组虐猫视频截图，一名时髦女子用高跟鞋将小猫踩死。不久，有网友发出“宇宙通缉令”，不少网友悬赏捉拿“凶手”。很快，该女子虐猫地点和她的工作单位等信息曝光。事件的结果是，虐猫女被解除职务。

四川地震

- 2008年5月21日，一段视频中一名女子用轻蔑的口气大谈对四川地震和灾区难民的看法，激烈和脏话充斥其中。随后，有网友发帖说，知道该女子的详细信息，包括身份证号、家庭成员、具体地址、QQ密码以及家人的电话。随后，警方将女子拘留，该女子向受害人道歉，但被人肉方未就信息泄露继续追责。

地铁骚扰事件

- 一段“地铁9号线男子摸女生大腿”的视频在网上热传，被骚扰的当事女乘客报案后男子否认骚扰行为。事件持续发酵后，多名网友公布了骚扰男及其妻女的照片、电话、住址、单位等具体信息。男子家庭被不断骚扰，男子最后不得不辞职。



陈某某人肉事件

- 2001年，有网民在猫扑网贴出一张“自己女朋友”的美女照片，引起网友关注并开始搜索。很快，这位名叫“陈某某”的女子大量个人资料被公布于网络，“陈某某事件”被视为人肉搜索的第一例，但那时候还没有“人肉”的说法。

死亡微博

- 北京一女白领跳楼身亡。她在“死亡博客”中将寻死原因归咎于丈夫的不忠，并在博客贴出丈夫和第三者的照片。随后，有网站将该女子丈夫的住址、工作单位等信息全部披露。部分网民到该女子丈夫和其父母住处骚扰。最终，法院宣判该女子丈夫起诉的三家网站赔偿8000元。

潘某某事件

- 14岁的潘某某因对足球球星出言不逊，结果手机、地址、学校、家人被一一曝光，更被粉丝上门围堵惊动警察，潘某某一度传出自杀。

- 杭州取快递女子被造谣出轨案、网红“罗小猫猫子”直播中喝农药自杀悲剧，再到寻亲男孩刘学州事件、上海女子200元打赏事件

寻亲之路遭遇网络暴力

刘学州4岁时，养父母遭遇烟花爆炸双双去世，年幼的他只能跟着姥姥一起生活。因为没有双亲，刘学州小时候经常被同村的孩子们欺负，被抢文具、被推搡、被诬陷，被骂是没人要的“野孩子”对于他不是父母亲生的这一点，姥姥从来没有隐瞒过，甚至在他表示想要找到亲生父母的时候也表示支持.....



在得知刘学州想和他们一起生活的时候，之前还言笑晏晏的亲生父母变了脸色，怒斥刘学州是他们生活的破坏者，“白眼狼”，无情的将他拉黑。



转发 186 评论 3174

赞 1.7万

1-24 00:02 Redmi K40

10.2万



薛定饿的狸花猫

所以去三亚旅游的钱跟生父母无关？

刘学州a : 无关!

共 460 条回复 >

1-19 13:36

115



生活在地府

所以你没钱咋还去三亚旅游，不理解。

-love-恶魔等人 共 360 条回复 >

1-19 13:32

192



孤舟一翁

穿着麦昆的鞋子去三亚旅游，然后哭诉自己没地方住，你也是够心机的👊

阿拉丁 sunny 芒等人 共 358 条回复 >

1-19 13:44

235



孤舟一翁

所以你到底让没让他们给你买房

活着要淡定等人 共 172 条回复 >

1-19 13:30

125

施暴者都是什么样的人？

- 网络暴力以辱骂、嘲讽、讥笑等形式伤害了不可计量的人，将许多事件推向了悲剧的结局。令人无奈的是，不少人对此习以为常，甚至参与到网络暴力中。
- 那么，这些施暴者都是些什么样的人呢？



键盘侠

部分在现实生活中胆小怕事，而在网上占据道德高点发表“个人正义感”和“个人评论”的人群

“键盘侠”：生活不如意，全靠网络治



“懂哥”：世上我最对，喷所有不同



“职业喷子”：专业施暴者，一切向钱看

这一类施暴者有自己的产业链、专业团队，从下单到售后，每一个环节都有明码标价，随时准备着当别人的打手

如何预防网络暴力?

■ 规范言行

- 控制自己在网络上的言行，文字，图片，语言，视频。防范网络暴力要**从我做起**，要从自己的网络行为做起。针对网络暴力我们要**规范自己的网络言行**。在网络上尽量运用规范的网络语言与理性网络行为，参与网络暴力防范与治理。而不是，与网络暴力与虎谋皮的参与网络暴力，成为网络暴力的施加者。

■ 洁身自好

- 与不健康的网站进行自我隔离，**不健康的朋友圈隔离，不健康的语言与行为隔离**。这是一个网民洁身自好的原则，也是一个具备是否分辨能力的网民，具备最起码的网络暴力**鉴别诊断能力**

■ 经受诱惑

- 要经受住诱惑，之所以强调要**经受住诱惑**。因为网络社会复杂，网络社会真假难辨，是否曲直很难确定。对此，作为新时代的网民，我们要经受住不良网站的黄色诱惑，经受住网络上的好奇事件的诱惑，经受住来此不同方向的兴趣与好奇心的诱惑

■ 法律保护

- 学会用法律保护自己，学用谦卑的语言与行为化解矛盾与暴力。如果，我们在网络上遭遇网络暴力对我们进行是假的暴力行为，我们要第一时间进行报警处理。**必要时自己要冷静，稳住自己的心情，控制自己的愤怒。把网络暴力者的信息与交谈内容保存下来，一做有力的证据**

■ 提升修养

- 要求提高自己的**网络道德修养**，提高自己的网络暴力防范意识。提高自己的网络文明行为，提高自己的控制能力与是否甄别能力

关于网络暴力的相关法律法规

关于办理信息网络实施诽谤等刑事案件的 司法解释

- 司法解释规定，利用信息网络诽谤他人，同一诽谤信息实际被点击、浏览次数达到**5000次以上**，或者被转发次数达到**500次以上**的，应当认定为刑法第246条第1款规定的“情节严重”，可构成诽谤罪；如果行为人明知是捏造的损害他人名誉的事实，实施了在信息网络上散布的行为，主观上故意，客观上造成实际损害，情节恶劣的，以诽谤罪定罪处罚。
- 《刑法》第246条诽谤罪，是指故意捏造并散布虚构的事实，足以贬损他人人格，破坏他人名誉，情节严重的行为。所谓情节严重，主要是指多次捏造事实诽谤他人的；捏造事实造成他人人格、名誉严重损害的；捏造事实诽谤他人造成恶劣影响的；诽谤他人致其精神失常或导致被害人自杀的等等情况。

日常网络安全

账号
密码
安全

病毒
风险
防范

网上
冲浪
安全

网上
交易
安全

电子
邮件
安全

主机
电脑
安全

办公
环境
安全

移动
手机
安全

无线
网络
安全

敏感
信息
安全

口令策略

一、以下哪个密码非常容易被破解？

- 1、cyh19930425
- 2、qwer1234!@#\$
- 3、Hisense\$%^&
- 4、639DCB74ed46!

三、当您收到一封邮件时，应当如何处理？

首先确认发件人信息首先确认发件人信息是否可信，确认身份后打开，若存在附件则查杀病毒后打开。

二、离开电脑时，锁定屏幕方法正确的是？

- 1、Ctrl键+L
- 2、Windows键+L
- 3、Alt+键L
- 4、关闭显示屏

四、当发现终端可能中病毒或存在异常时候，您应当如何处理？

将设备异常信息主动上报安全部门，协助安全部门对重点进行排除处置。

口令策略

选择易记强口令的几个窍门:

- 一句话记忆（名言、诗句、歌词）+数字/字母
- 使用叠词：提取首字母，再把叠词变为数字
- 用数字和符号替换

密码：Quit@smoking4ever

解释：永远戒烟

密码：flzx3qcysyhl9t

解释：飞流直下三千尺疑是银河落九天

密码：Travel-777-Xiecheng

解释：单词-数字-网站名称

密码：1dcypsz1/2jss1/2j#f00

解释：一道残阳铺水中，半江瑟瑟半江红

密码：wmyqxmjyqM*5

解释：我们一起学猫叫，一起喵喵喵喵

密码：SjdDfzr0101~

解释：神即道，道法自然+特殊日期



账号密码安全

01 如果有初始密码,应尽快修改

02 密码长度不少于8个字符

03 不要使用单一的字符类型,例如只用小写字母,或只用数字

04 用户名与密码不要使用相同字符

05 常见的弱口令尽量避免设置为密码

06 自己、家人、朋友、亲戚、宠物的名字避免设置为密码

07 生日、结婚纪念日、电话号码等个人信息避免设置为密码

08 工作中,用到的专业术语、职业特征避免设置为密

码

09 密码字典中不应包含单词,或者在单词中插入其他字符

10 所有系统尽可能使用不同的密码四防止网页自动记住账号密码

11 防止网页自动记住账号密码

12 上网注册帐户时,用户名密码不要与公司内部用户名密码相同或有关联

13 在通过密码管理软件保管好密码的同时,密码管理软件应设置高强度安全措施

14 密码应定期更换



计算机中毒症状

- ✓ 计算机速度变慢，出现蓝屏甚至死机
- ✓ 程序载入的时间变长
- ✓ 可执行程序文件的大小改变了
- ✓ 没有存取磁盘，但磁盘指示灯却一直在亮
- ✓ 开机后出现陌生的声音、画面或提示信息，以及不寻常的错误信息或乱码
- ✓ 系统内存或硬盘的容量突然大幅减少
- ✓ 文件的内容改变或被加上一些奇怪的资料，或文件离奇消失



病毒风险防范

15 安装病毒防护程序并及时更新病毒特征库

16 下载电子邮件附件时注意文件名的后缀,陌生发件人附件不要打开

17 网络下载的文件需要验证文件数字签名有效性,并手动扫描文件

18 使用移动存储介质时,进行查杀病毒后打开

19 安装不明来源的软件时,手动查杀病毒

20 浏览网页时, 计算机使用过程中发现异常,断开网络全盘杀毒



网上冲浪安全

- 21 使用知名的安全浏览器
- 22 收藏经常访问的网站,不要轻易点击别人传给你的网址
- 23 对超低价、超低折扣、中奖等诱惑要提高警惕
- 24 避免访问色情、赌博、反动等非法网站**
- 25 重要文件通过网络、邮件等方式传输时进行加密处理
- 26 利用社交网站的安全与隐私设置保护敏感信息**
- 27 避免将工作信息、文件上传至网上存储空间,如网盘、云共享文件夹等**
- 28 在社交网站谨慎发布个人信息**
- 29 根据自己对网站的需求进行注册,不要盲目填写信息
- 30 上网的DNS应设置为运营商指定的或内部DNS服务的IP地址,避免使用不安全的DNS导致被劫持风险



网上交易安全

31 所访问的网址与官方地址进行比对,确认准确性

32 避免通过公用计算机使用网上交易系统

33 不在网吧等多人共用的电脑上进行金融业务操作

34 不通过搜索引擎上的网址或不明网站的链接进入交易

35 在网络交易前,对交易网站和交易对方的资质全面了解

36 可通过查询网站备案信息等方式核实网站资质真伪

37 应注意查看交易网站是否为HTTPS协议,保证数据传输中不被监听篡改

38 在访问涉及资金交易类网站时,尽量使用官方网站提供的虚拟键盘输入登录和交易密码

39 填写个人详细信息可获得优惠券,要谨慎填写

40 注意保护个人隐私,使用个人的银行账号、密码和证件号码等敏感信息时要慎重

41 使用手机支付服务前,按要求在手机上安装专门用于安全防范的插件

42 无论以何种理由要求你把资金打入陌生人账户、安全账户的行为都是诈骗犯罪,切勿上当受骗

43 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

电信诈骗事件

近日，葛同学用手机上网时，看到一个自称可办理计算机二级合格证书、英语四级合格证书的帖子。随后，小葛便按照联系方式添加了对方的微信。当日，葛同学就接到自称办理计算机二级合格证书、英语四级合格证书操作人贾老师打来的电话和发来的微信，对方要求葛同学缴纳1000元操作费、3000元办证费、50元寄递费、600元订金。在葛同学一番诉苦博得贾某同情后，按照对方指示先通过微信转账订金，经商定事成再将剩余的操作费、办证费、寄递费一并转账。成功缴纳定金后，贾某瞬间将葛某微信拉黑，此时葛同学拨打这个贾某电话已处于关机状态。



提醒

在许多大学，取得计算机和英语等级证书，是顺利毕业以及尽快就业的前提。为了顺利拿到这些证书，一些大学生便四处寻找“捷径”。骗子正是利用学生这种急于求成的心理，将其引入设计好的套中。此类案件，嫌疑人主要通过打电话、发短信、网络传播等渠道，以办理各种合格证书为理由，向被害人收取各种手续费、服务费，大学生要警惕这些作案手法，提高警觉性，以正当的途径获取证书与奖励。

不法分子利用学生防范心理弱的特点，诱导学生扫二维码，学生在不知情的情况下，登录预设网站自动下载木马病毒，导致个人信息，网银密码等被盗窃。学生小王在某个街口因为贪图送的小礼品扫描了陌生的二维码，结果回到家发现自己的支付宝被五次盗刷，总共被盗走1500元，等到发现的时候已经晚了。



提醒

面对扫描二维码打折优惠促销等活动，要提高警惕，不要见码就扫，建议在手机上安装防病毒安全软件。

电信诈骗事件

近日，陈同学在一家网店购买一台标价为5700元的笔记本电脑，但因操作失误多付了一次款。因退款心切，在客服的要求下，陈同学加了对方QQ，让对方远程操控自己的电脑“帮助退款”，结果被对方分3次转走一万余元。



提醒

千万不要让陌生人远程操作你的电脑。因为一旦启动远程操控，任何人都可以在异地通过网络控制你的电脑。另外，网购交易需要加QQ沟通的，往往是诈骗。

张同学收到某银行官方号码“95xxx”发来的短信，提示她银行卡积分将于近期到期，建议尽快登录某网站兑换礼品，并附上了网站链接。

张同学完全没有质疑该网址的可靠性，直接通过手机登录，并按照规定输入了个人信息、账号及密码。不久，她就收到银行发来的短信，提示她的银行卡被取现4000元。



提醒

不要轻易点击任何信息发来的链接，获奖等信息应当搜索官方渠道确认后再进行操作。

电子邮件安全

44 不打开、回复可疑邮件、垃圾邮件、不明来源邮件 须进行帐号密码验证

45 收发公司业务数据时，必须使用公司内部邮箱，公务处理和私人邮箱分开

46 员工应对自己的邮箱账号和密码的安全负责，不得将邮箱账号借与他人

47 若发现邮箱存在任何安全漏洞的情况，应及时通知公司邮件系统管理人员

48 应警惕邮件的内容、网址链接、图片等

49 机关工作人员工作邮件建议使用政府自建邮箱，严禁使用境外邮箱

50 为电子邮箱设置高强度密码，并设置每次登陆时必

51 开启防病毒软件实时监控，检测收发的电子邮件是否带有病毒

52 检查邮件转发功能是否关闭

53 不转发来历不明的电子邮件及附件

54 收到涉及敏感信息邮件时，要对邮件内容和发件人反复确认，尽量进行线下沟通



主机电脑安全

55 操作系统应及时更新最新安全补丁

56 禁止开启无权限的文件共享服务，使用更安全的文件共享方式针对中间件、数据库、平台组件等程序进行安全补丁升级

57 针对中间件、数据库、平台组件等程序进行安全补丁升级

58 关闭办公电脑的远程访问定期备份重要数据

60 关闭系统中不需要的服务回

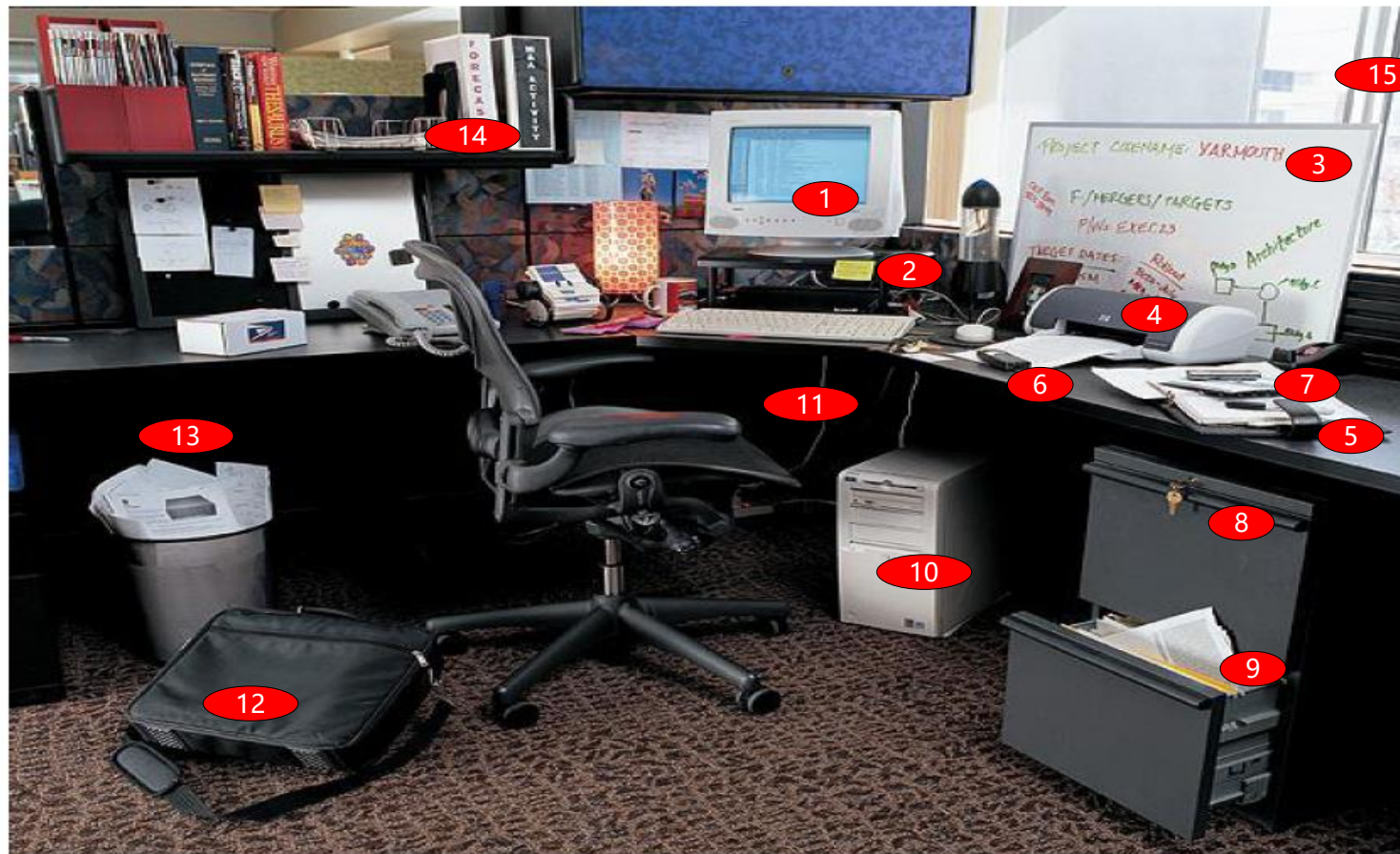
61 计算机系统更换操作人员时，交接重要资料的同时，更改该系统的密码

62 及时清理垃圾箱

63 员工离开座位时应设置电脑为退出状态或锁屏状态，建议设置自动锁屏



办公环境



办公环境安全

64 禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需用碎纸机粉碎

65 废弃或待消磁介质转交他人时应经管理部门消磁处理

66 离开座位时，应将贵重物品、含有机密信息的资料锁入柜中

67 应将复印或打印的资料及时取走

68 废弃的光盘、U盘、电脑等要消磁或彻底破坏

69 禁止在便签之上写有账号、密码等信息

70 UKey不使用时应及时拔出并妥善保管

71 办公中重要内容电话找到安全安静的地方接听，避免信息泄露

72 U盘、移动硬盘，随时存放在安全地方，勿随意借用、放置



移动手机安全

**73 手机设置自动锁屏功能，建议设置1-5分钟的，避免 81 手机废弃前应对数据进行完全备份，恢复出厂设置
离开手机后被其他人恶意使用 清除残余信息**

74 手机升级应通过自带的更新功能，避免通过网站下载更新

82 经常查看手机任务管理器，检查是否有恶意程序在后台运行，并定期使用手机安全系统软件扫描手机系统

75 尽可能通过手机自带的应用市场下载手机应用程序

83 对程序执行权限加以限制，非必要程序禁止读取通讯录等敏感数据

76 为手机安装杀毒软件

77经常为手机做数据同步备份

84 不要试图破解自己的手机，以保证应用程序的安全性

78 手机中访问Web站点应提高警惕

**79 为手机设置访问密码是保护手机安全的第一道防线，
防止手机丢失信息泄露**

80 蓝牙功能不用时，应处于关闭状态



无线网络安全

85 在办公环境中禁止私自通过办公网开放Wi-Fi热点

86 不访问任何非本单位的开放Wi-Fi，发现单位附近的无密码、开放的Wi-Fi应通知IT部门

87 除测试、安全、移动端外，其他部门需求Wi-Fi需要报备IT部门，不许自行开热点

88 禁止使用Wi-Fi共享类APP，避免导致无线网络账号密码泄露

89 无线网络设备及时更新到最新固件

90 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

91 设置高强度的无线密码，各单位的认证机制建议采取实名方式



敏感数据安全

92 敏感及内网计算机不允许连接互联网或其它公共网络

93 处理敏感信息的计算机、传真机、复印机等设备应当在单位内部进行维修,现场有专门人员监督

94 严禁维修人员读取或复制涉密信息,确定需送外维修的,应当拆除涉密信息存储部件

95 敏感信息设备改作非涉密信息设备使用或淘汰时,应当将涉密信息存储部件拆除

96 敏感及内网计算机不得使用无线键盘、无线鼠标、无线网卡敏感文件不允许在非涉密计算机上进行处理

98 内外网数据交换需使用专用的保密U盘或刻录光盘

99 工作环境外避免透露工作内容

100 重要文件存储应先进行加密处理



社会工程学

通过对受害者**本能反应、好奇心、信任、贪婪等心理弱点**进行如欺骗和伤害等攻击手段。

在信息安全这个链条中，人的因素是最薄弱的一环。
社会工程就是利用人的薄弱点，通过欺骗手段而入侵计算机系统的一种攻击方法。

攻击方式主要包括三个方面！



■ 如何防范社会工程学？

- ✓ 不要轻易泄漏敏感信息，例如口令和账号
- ✓ 在相信任何人之前，先校验其真实的身份
- ✓ 不要违背公司的安全策略，哪怕是你的上司向你索取个人敏感信息（黑客最擅长的就是冒充一个很焦急的老板，利用一般人好心以及害怕上司的心理，向系统管理员索取口令）
- ✓ 不要忘了，所谓的黑客，更多时候并不是技术多么出众，而是社会工程的能力比较强

**网络安全为人民
网络安全靠人民**

