中国·郑州 2020
CHINA ZHENGZHOU China Cybersecurity Week

国家网络安全宣传周

网络安全为人民 网络安全靠人民

郑州市网络安全科普教育基地

网络安全手册

2020年9月
中国·郑州

指导单位：2020年国家网络安全宣传周郑州市筹备工作领导小组
主办单位：郑州市科学技术协会、郑州市郑东新区管理委员会
承建单位：中科院计算技术研究所大数据研究院

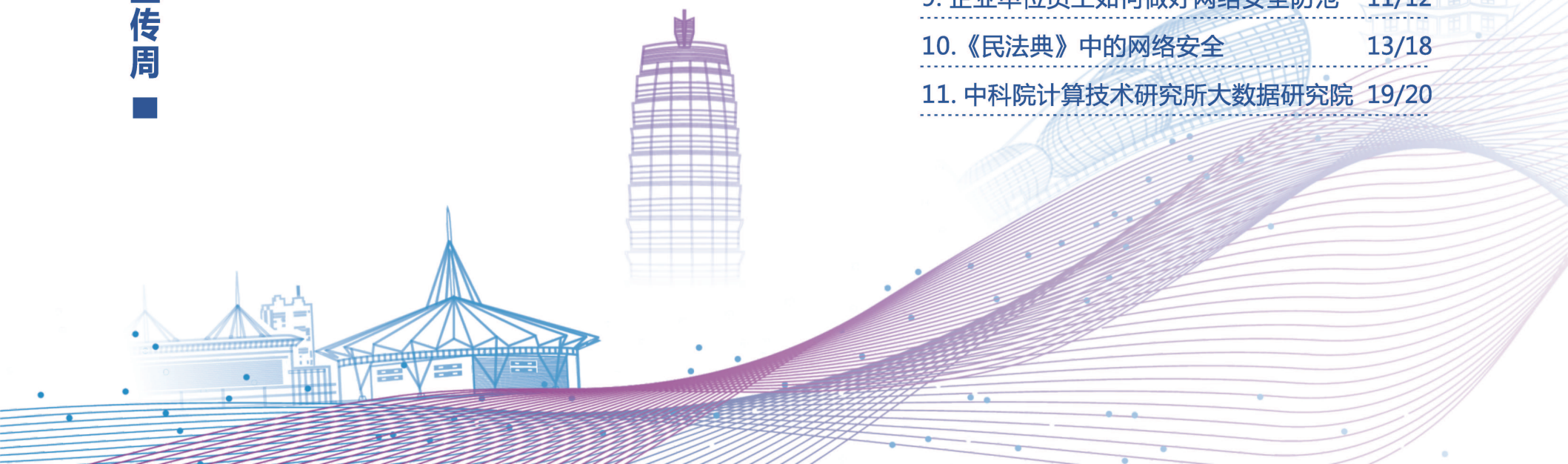
国家网络安全宣传周
China Cybersecurity Week

中国·郑州
CHINA ZHENGZHOU
2020
China Cybersecurity Week

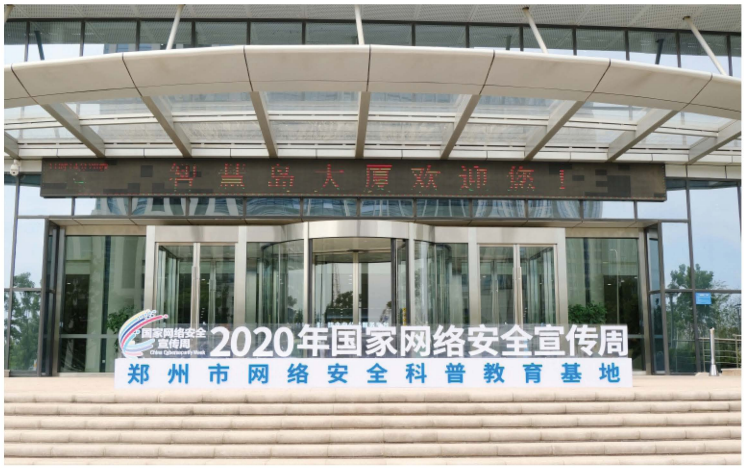
国家网络安全宣传周

目录 CATALOGUE ▼

1. 郑州市网络安全科普教育基地 01/02
2. 2020上半年十大网络安全事件 03/05
3. 如何正确使用网络 06
4. 如何防止个人隐私泄露 06
5. 如何防止黑客入侵你的手机 06
6. 如何防范电信诈骗 07
7. 如何防止网络常见诈骗行为 07/08
8. 青少年如何做好网络安全防范 09/10
9. 企业单位员工如何做好网络安全防范 11/12
10.《民法典》中的网络安全 13/18
11. 中科院计算技术研究所大数据研究院 19/20



2020年国家网络安全宣传周
郑州市网络安全科普教育基地



2020年国家网络安全宣传周（简称"网安周"）将于2020年9月在郑州举办，本届网安周以“网络安全为人民 网络安全靠人民”为主题，围绕金融、电信、环保、交通、人工智能、大数据等重点领域和行业网络安全问题，针对社会公众关注的热点问题，成立2020年国家网络安全宣传周郑州市网络安全科普教育基地（下称“基地”），并于8月4日由河南省委网信办主任郭岩松，郑州市委常委、宣传部长黄卿，中科院计算技术研究所副所长、研究员程学旗等共同揭牌。

基地由2020年国家网络安全宣传周郑州市筹备工作领导小组指导，郑州市科学技术协会、郑州市郑东新区管理委员会主办，中科院计算技术研究所大数据研究院承建，设立了网络安全主题展厅、网络安全互动体验厅、网络安全沉浸式体验厅等展区，将在活动期间开展网络安全科普大讲堂等系列活动。

基地通过数据安全攻防实物体验、人人编程互动体验、沉浸式观影体验、短信嗅探、无线监听、态势感知等高科技体验，网络安全知识问答、网络安全大讲堂等科普活动，从多个维度、不同视角向公众进行通俗易懂的网络安全知识介绍、解读和普及，提升公众网络安全防护技能。

预约入口

开放预约

活动期间，设在中科院计算技术研究所大数据研究院的2020年国家网络安全宣传周郑州市网络安全科普教育基地已面向公众定时开放，可通过“中科院计算所大数据研究院”公众号预约个人/团体参观基地的日期、场次及人数。同时，将长期开展网络安全大讲堂活动，具体展出和活动时间请持续关注我们。

基地地址：郑州市郑东新区中道东路6号智慧岛大厦8F

2020上半年十大网络安全事件

1. 美天然气管道商遭攻击，被迫关闭压缩设施

2020年2月，美国国土安全部的网络安全和基础设施安全局发布公告，一家未公开名字的天然气管道运营商，在遭到勒索软件攻击后关闭压缩设施达两天之久。攻击事件发生的具体时间未获公布。

据悉，攻击始于钓鱼软件内的恶意链接，攻击者从IT网络渗透到作业OT网络，并植入勒索软件。在关闭压缩设施期间，由于管道传输的依赖性，连带影响到了其他地方的压缩设施。

2. 以色列供水部门工控设施遭到网络攻击

2020年4月，以色列国家网络局发布公告称，近期收到了多起针对废水处理厂、水泵站和污水管的入侵报告，因此各能源和水行业企业需要紧急更改所有联网系统的密码，以应对网络攻击的威胁。

以色列计算机紧急响应团队(CERT)和以色列政府水利局也发布了类似的安全警告，水利局告知企业“重点更改运营系统和液氯控制设备”的密码，因为这两类系统遭受的攻击最多。

3. 丹麦水泵制造商DESMI遭网络攻击

2020年4月12日，全球水泵制造商DESMI表示，该公司网络和运营系统遭受攻击，在安全事件发生后，该公司恢复其IT系统。攻击发生4月9日晚上，正值新冠病毒大流行期间，公司员工在家中工作。网络攻击后，公司的所有系统都已关闭。DESMI已经向当局和丹麦警方报告了这一事件。DESMI宣布将尽快向所有客户和业务合作伙伴提供更新。

4. 欧洲能源巨头EDP遭网络攻击，被勒索近1000万欧元

2020年4月，葡萄牙跨国能源公司EDP(Energias de Portugal)遭到勒索软件攻击。攻击者声称，已获取EDP公司10TB的敏感数据文件，并且索要了1580的比特币赎金(折合约1090万美元/990万欧元)。

EDP集团是欧洲能源行业（天然气和电力）最大的运营商之一，也是世界第四大风能生产商，在全球四个大洲的19个国家/地区拥有业务。

5. 可编程门阵列（FPGA）芯片被发现潜在严重漏洞，或使许多任务关键型和安全关键型设备遭受攻击

2020年4月22日，研究人员在现场可编程门阵列（FPGA）芯片中发现了一个潜在的严重漏洞，该漏洞可能使许多任务关键型和安全关键型设备遭受攻击。FPGA是安全组件并且可在现场进行编程，存在于各种系统中，包括工业控制系统（ICS）、云数据中心、蜂窝基站、医疗设备和航空系统。为利用该漏洞，攻击者需要访问目标设备的JTAG或SelectMAP接口，但研究人员警告称，也有可能实现远程攻击。该漏洞已于2019年9月报告给供应商并被确认存在，如不更换硅，就无法修补该漏洞。此外，他们指出，Xilinx的新型UltraScale和UltraScale+芯片正在慢慢取代旧型号，因此不容易受到攻击。

6. 委内瑞拉国家电网干线遭攻击全国大面积停电

2020年5月5日，委内瑞拉副总统罗德里格斯宣布消息，委内瑞拉国家电网干线遭到攻击，造成全国大面积停电。委国家电力公司组织人力全力抢修，部分地区已经恢复供电。

罗德里格斯表示，国家电网的765干线遭到攻击。这也是在委挫败雇佣兵入侵委内瑞拉数小时后发生的。除首都加拉加斯外，全国11个州府均发生停电。

7. 澳大利亚航运及物流公司Toll集团4个月内两次遭到攻击

日前，澳大利亚航运及物流公司Toll集团遭到勒索软件攻击，随后该公司便清理服务器，防止数据被盗。据悉，这是四个月内Toll集团遭遇的第二次勒索软件攻击，另一次攻击事件发生在今年2月份。

经调查发现，被攻击系统中存在Nefilim勒索软件（由Nemty演变而来的新一代勒索软件），该勒索软件会利用暴露在外的远端桌面（RDP）连接埠进行散播，并使用 AES-128 加密来锁定文件。在盗走企业资料后，不法分子会以公布机密资料作为理由来勒索企业。

8. 台湾两大炼油厂遭受勒索软件攻击，加油站混乱

2020年5月，台湾石油，汽油和天然气公司CPC公司及其竞争对

手台塑石化公司（FPCC）在过去两天内都受到了网络攻击。

CPC首先受到攻击，而FPCC在第二天也遭受攻击。5月4日，对CPC的攻击使其IT和计算机系统关闭，加油站无法访问用于管理收入记录的数字平台。

尽管仍接受信用卡和现金，但客户无法在加油站使用VIP支付卡或电子支付应用程序。CPC高管声称，破坏是由勒索软件引起的。

9. 瑞士铁路机车制造商Stadler遭到网络攻击

2020年5月9日，瑞士铁路机车制造商Stadler对外披露，于近期遭到了网络攻击，攻击者设法渗透了它的IT网络，并用恶意软件感染了部分计算机，很可能已经窃取到部分数据。未知攻击者试图勒索Stadler巨额赎金，否则将会公开所窃得的数据。

Stadler是机架铁路车辆的全球领先制造商，主营产品包括高速火车，城际火车，区域火车和S-Bahn火车，地下火车，电车火车和有轨电车。该公司声称已针对该事件展开调查，并拒绝支付赎金，通过重新启动受影响系统，运行备份系统恢复运营。

10. 本田汽车遭受工业型勒索软件攻击，部分生产系统中断

2020年6月8日，日本汽车制造商本田（Honda）表示，其服务器受到Ekans勒索软件攻击后，正在应对网络攻击。该事件正在影响公司在全球的业务，包括生产。

本田随后在一份声明中说：“本田可以确认本田网络发生了网络攻击。该问题正在影响其访问计算机服务器，使用电子邮件以及使用其内部系统的能力。此外对日本以外的生产系统也有影响。目前正在开展工作以最大程度地减少影响并恢复生产，销售和开发活动的全部功能。”

如何正确使用网络？

1、不能危害网络安全。
2、不能为危害网络安全的活动提供工具及帮助。
3、不能危害国家安全、荣誉及利益。
4、不能煽动颠覆国家政权，推翻国家政权制度。
5、不能煽动分裂国家，破坏国家统一。
6、不能宣扬恐怖主义，极端主义。
7、不能宣扬民族歧视，民族仇恨。
8、不能传播暴力，淫秽色情信息。
9、不能编造，传播虚假信息扰乱经济秩序和社会秩序。
10、不能侵犯他人名誉、隐私、知识产权。

如何防止个人隐私泄露？

1、网络购物要谨防钓鱼网站。
2、妥善处置含个人信息的单据。
3、身份证复印件上要写明用途。
4、简历只提供必要信息。
5、不在微博、群聊中透露个人信息。
6、微信不要加不明身份的好友。
7、慎重参加网上调查活动。

如何防止黑客入侵你的手机？

1、一定要为你的手机设定密码。
2、使用正版的购物App。
3、不要让手机的App或者用浏览器时记录帐号密码。
4、关掉自动跳转Wifi功能。
5、别随时把蓝牙装置打开。
6、智能手机出售要恢复原厂。
7、谨慎下载App软件。
8、定期清除浏览记录。
9、下载远端清除软件。

如何防范电信诈骗？

1、不要轻易泄露个人信息，特别是姓名、身份证号、银行卡信息，绝对不能同时公布上述三种号码。

2、不要急于汇款，要认真查看来电号码，当不能辨别信息真假时，要在第一时间拨打相关查询电话。

3、不要轻易将资金转入陌生人账户，汇款前多方确认该人身份。

4、不要用手机回拨电话，为防范犯罪分子使用虚拟手机号码冒充专业部门电话，机主最好找固定电话或其他电话进行确认。

5、不要轻易相信网络、短信等提供的信息。不要因贪小利而受违法短信的诱惑。

6、不要在慌乱中作出决断，心态要保持平静。

如何防止网络常见诈骗行为？

1、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，淘宝交易需要加QQ沟通的，往往是诈骗。

2、小心别中钓鱼链接的招。网络购物，尤其付款时，务必仔细核对网址，认清购物网站的域名，不要轻易点击对方发来的链接。

3、务必保护好账户、密码、验证码等信息。当对方试图索取密码、手机校验码等信息时，十有八九是骗子，一定要提高警惕，千万不要透露。

4、网上购物请选择正规网站，不要轻信虚假网站、QQ、论坛等发布的所谓超低价促销信息。此外，要求通过银行等直接汇款的 9 成以上为诈骗，务必警惕。

5、要警惕收到的陌生邮件、文档、链接，不要轻易点击，防止木马病毒。如遇疑难问题，一定要找官方客服了解咨询，或拨打110求助。

6、淘宝交易流程不存在没有保证金便无法付款的情况。此外，卖家可上淘宝论坛学习如何识别真假网址及客服。

7、关于刷信誉类信息，请不要回复和轻信。尤其是让卖家先行付款的操作模式，十有八九是诈骗，钱款一旦支付，无法追回。而且淘宝杜绝刷信誉，请卖家诚信经营。

8、骗子以“回扣”之名，要求转账，钱直接进入对方账户，而支付宝订单，买家则可以申请退款。所以交易时，千万不要通过支付宝等直接转账，一旦转账，损失就无法挽回。

9、仅通过QQ或者电话联系的招聘往往是诈骗，需要你先掏钱的往往是诈骗。这些需要“刷信誉”的网站实际上都是一些无法退款的虚拟商品交易网站，一旦被骗，投诉无门。

10、无论是给你打钱还是向你借钱，如在网上提出钱财交易请求，即便有视频画面也不要轻信，务必先打电话确认；同时要牢记，手机上收到的验证码，千万不能随意泄漏。

11、目前，各类金融投资类钓鱼网站已成欺诈主流之一，所谓的“会员制”、“天天返利”、“高额回报”、“翻倍分红”实为欺诈，一旦败露，骗子就关闭网站，遁逃无踪。

12、请通过正规渠道贷款、办理信用卡。切勿轻信“无抵押贷款”、“办理信用卡”、“网络中奖”等诱惑性信息，需要你先拿出钱财的一定要警惕。

青少年如何做好网络安全防范

网络知识素养是现代家庭教育的新内容。保护未成年人权益，应科学系统推动未成年人新媒体素养教育。所以，我们选取了一些常见的涉及网络安全的几个方面，希望能起到提高青少年安全意识、增强自我保护技能的作用。

一、微信朋友圈禁止陌生人查看照片

微信在未成年人常用网络社交工具和应用中占11.8%，很多人已经习惯在微信上记录自己生活中的一切。

尽管“朋友圈”只有好友才能看和评论你分享的照片，然而这个相对封闭的圈子却留有一扇“后门”，一旦“附近的人”被启用，即便不是微信好友，你的10张照片也会被非好友的陌生人尽收眼底。以朋友圈为例，首先点击“找附近的人”功能，然后选择“清除位置信息并退出”。最后在设置项，关掉“允许陌生人看10张照片”的隐私设置。

二、小心微博相册、签到、足迹

调查显示，超过六成的青少年(61.6%)使用微博，高于整体网民(54.7%)。未成年人在进行网上交友时，32.3%会公布真实姓名，公布学校名称(20.9%)、电子邮箱(18.4%)、照片(15.5%)、班级(12.1%)、手机号(7.3%)等易直接定位和识别的个人信息者也有相当比例。

大家在网上晒快乐的同时别忘了保护自己隐私，不要在微博等线上平台上泄露出游时间、人数等信息。如果要发布的话最好也是对现实好友分组可见。

三、慎用公共场所免费网络

现在青年人聚会，到了餐厅或者咖啡馆，要做的第一件事往往是拿出手机搜索免费无线网络。

一些不法分子就是利用这一点，在公共场所用一台电脑、一套无线网络及一个网络包分析软件就搭建了一个不设密码的wifi。如用户使用该wifi，不法分子就可以盗取手机上的资料。在一些公共区域，尽量不使用带有个人帐号和密码信息的软件。

四、小心恶意软件

现在网络搜索很方便，但是过于方便的同时也意味着信息量庞大而难以甄别，在下载软件前最好先做调查、看评论，避免进入不合法的软件站点下载，最好使用新版的反病毒软件。这些恶意软件可在后台收集用户的位置信息、通话记录、电话号码及短信等信息并将其上传至指定服务器，造成难以估量的危害。

五、禁用游戏内置收费项目

很多青少年甚至成年人逐渐已经习惯在闲暇时通过自己的移动终端来进行游戏娱乐，但是玩游戏的同时也有几点要注意。不要把银行卡跟账户相关联。很多扣费代码是内置在游戏中，不用通过用户审核便直接扣费。用户在遭到恶意扣费以后不会收到提示消息，而只能通过查询电话消费记录方可知道，这对于一般不会查询账单的用户来说便无从所知。

六、网络购物应谨慎

享受网购便利的同时不要忘记以下几点：一定要通过第三方交易平台支付；认真核查卖家信誉度，不要被刷出来的高信誉所迷惑；不要被低价迷花眼，要牢记天上不会掉馅饼；票据、聊天记录要保存；收货后要当面拆开确认。

企业单位员工如何做好网络安全防范

一、常见病毒与危害

计算机病毒通常分为引导型、文件型、网络型。勒索病毒(Ransomware)是近年常见并颇具危害性的一种计算机病毒，其通过加密手段绑架用户文件或数据，并以此向用户勒索钱财。导致用户或文件数据不可恢复，系统无法运行，造成损失。

安全提示: 1、及时更新补丁。2、做好文件备份。3、安装防病毒软件。4、不点击不可信链接、不下载不可信文件、不打开不可信电子邮件。

二、病毒防范

1、办公终端必须安装企业统一部署的防病毒软件，及时更新病毒库。
2、使用移动存储设备时，应先运行防病毒软件进行病毒扫描。

三、如何应对电脑感染病毒

1、迅速断开计算机与所有网络的连接。
2、联系专业人员进行处理。

四、终端安全管理软件

1、办公终端安装企业统一部署的桌面安全管理软件。
2、根据提示完成用户身份认证，准确填写用户信息，以便及时获取协助。
3、不违规禁用或卸载终端安全管理软件。

五、正确设置、使用密码

1、密码的长度应至少8个字符，并采用大写字母、小写字母、数字、符号中选择三种相组合的方式。
2、不要把密码写在纸上，密码应每隔3个月变更一次，最近5次密码不能相同。
3、一定要立即更改系统的初始化密码。
4、工作电脑中所使用的密码不要与个人电脑中使用的密码相同。

六、离开电脑锁屏或关机

离开电脑一定要记得按下WIN+L键锁屏，或关闭电脑。

七、软件卸载、下载、安装

1、不私自卸载公司统一安装部署的软件。
2、不随意下载软件进行安装。
3、应使用正版授权的软件。

八、网络安全接入

1、网络准入系统会要求用户接入网络时进行实名认证和合规检查。
2、对不合规的终端，系统会自动引导用户进行修复。

九、网页浏览安全

1、不浏览不良信息网站。
2、及时清理浏览器历史记录和缓存。

十、邮件安全

1、不随意发送内部敏感信息。
2、不轻易接受陌生的链接及下载项。

十一、合理使用移动介质

1、及时清理移动介质中的文件，敏感文件使用后立即删除。
2、不将私人信息移动介质与工作信息移动介质混用。

十二、关闭移动介质自动播放功能

确保在计算机设置中，关闭移动介质的自动播放功能。

十三、移动设备安全

1、谨慎安装移动设备应用程序，尽量从官网下载安装。
2、使用安全的密码对移动设备进行保护。
3、利用杀毒软件保护移动设备。

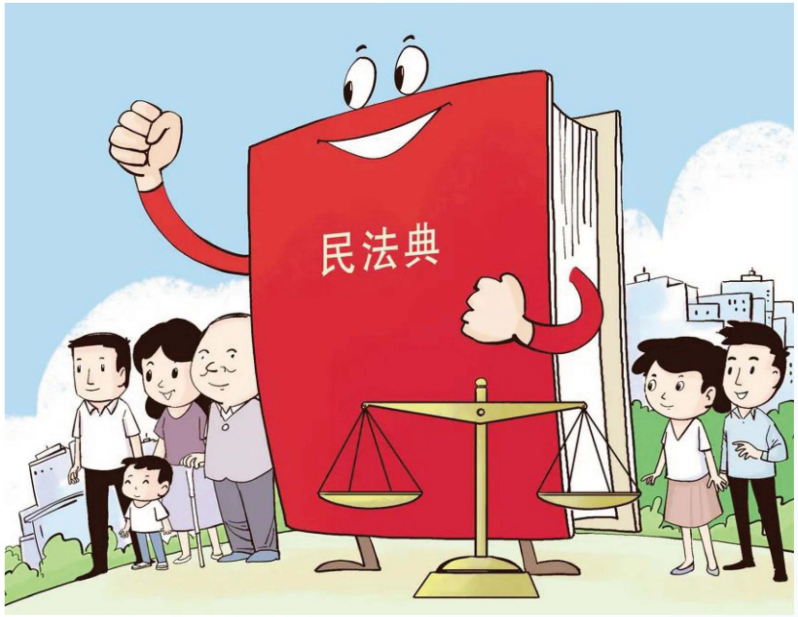
十四、重要数据备份

重要数据一定要定期备份！

《民法典》中的网络安全

2020年5月28日，新中国首部《民法典》正式通过。

《民法典》被称为“社会生活的百科全书”，是一个国家经济社会发展的真实写照。当下，中国正经历着以大数据、5G等新技术新产业为标志的第四次工业革命，民事权利义务关系正发生着重大变革。在此背景下，《民法典》如何回应互联网时代的特殊要求？我们看到，人格权独立成编，强化对隐私权和个人信息的保护；侵权责任编对网络侵权责任进行了完善……为更好地理解《民法典》关于网络安全的规定，我们对相关条文进行了梳理和解读，带大家读懂《民法典》中的网络安全。



一、隐私权和个人信息保护

1、明确隐私权和个人信息的定义

- 首次明确了隐私的定义

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。(第一千零三十二条)

- 规制了隐私权侵害行为

除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁；进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；拍摄、窃听、公开他人的私密活动；拍摄、窥视他人身体的私密部位；处理他人的私密信息；以其他方式侵害他人的隐私权。(第一千零三十三条)

- 界定了个人信息的定义

个人信息是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的各种信息。（第一千零三十四条）

- 列举了个人信息的范围

比《网络安全法》规定的个人信息范围多了“电子邮箱”、“健康信息”、“行踪信息”三项。（第一千零三十四条）

- 明确了个人信息保护与隐私权的关系

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。(第一千零三十四条)

2、 规定处理个人信息应遵循的原则和条件

- 处理个人信息应遵循的原则

合法、正当、必要，不得过度处理。

- 处理个人信息应遵循的条件

征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；公开处理信息的规则；明示处理信息的目的、方式和范围；不违反法律、行政法规的规定和双方的约定。

- 明确个人信息的处理的内涵

包括个人信息的收集、存储、使用、加工、传输、提供、公开等。(第一千零三十五条)

3、规定处理个人信息的免责情形

处理自然人个人信息，应当严格遵循法定的原则和条件进行，但以下情况可以免责:

● 在该自然人或者其监护人同意的范围内合理实施的行为。

● 合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。

● 为维护公共利益或者该自然人合法权益，合理实施的其他行为。(第一千零三十六条)

4、规定个人信息主体的权利

● 查阅权、复制权

自然人可以依法向信息处理者查阅复制其个人信息。

● 更正权

自然人发现信息有错误的，有权向信息处理者提出异议并请求及时采取更正等必要措施。

● 删除权

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。(第一千零三十七条)

5、信息处理者的信息安全保障义务

● 不得泄露、篡改

信息处理者不得泄露、篡改收集、存储的个人信息。

● 不得向他人非法提供

信息处理者未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

● 保护信息安全

信息处理者应当采取技术措施和其他必要措施确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失。

● 补救措施及报告制度

发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。(第一千零三十八条)

6、强化未成年人个人信息的保护

对未成年人的个人信息的处理，增加“征得监护人同意”的规定，但是法律、行政法规另有规定的除外。(第一千零三十五条)

7、国家机关、承担行政职能的法定机构及其工作人员的保密义务

规定了国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。(第一千零三十九条)

二、其他涉及网络安全的人格权

1、 虚拟身份受法律保护

网名、笔名等并非自然人的真实姓名，而是自然人的虚拟身份。虚拟身份具有一定社会知名度，被他人使用足以造成公众混淆的，参照适用姓名权和名称权保护的有关规定。(第一千零一十七条)

2、 防止“深度伪造”侵犯肖像权、声音权

利用信息技术手段“深度伪造”他人的肖像、声音，不仅侵害自然人的人格权益，还可能造成恶劣社会影响，危害国家安全和社会公共利益。

《民法典》规定，不得以利用信息技术手段伪造等方式侵害他人的肖像权。(第一千零一十九条)

对自然人声音的保护，参照适用肖像权保护的有关规定。(第一千零二十三条)

3、 规制网络等媒体的名誉侵权行为

针对网络等媒体报道的内容失实，侵害名誉权行为，《民法典》规定受害人有权请求媒体及时采取更正或者删除等必要措施。前提是民事主体有证据证明侵害行为的发生。(第一千零二十八条)

三、网络侵权责任

1、确定了权利人通知、网络服务者转通知、网络用户声明、网络服务提供者转声明等规则，细化了程序和证据方面的规定：

● 权利人通知规则

网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。通知应当包括构成侵权的初步证据及权利人的真实身份信息。因错误通知造成网络用户或者网络服务提供者损害的，应当承担侵权责任。法律另有规定的，依照其规定。

● 网络服务者转通知规则

网络服务提供者接到通知后，应当及时将该通知转送相关网络用户，并根据构成侵权的初步证据和服务类型采取必要措施；未及时采取必要措施的，对损害的扩大部分与该网络用户承担连带责任。(第一千一百九十五条)

● 网络用户声明规则

网络用户接到转送的通知后，可以向网络服务提供者提交不存在侵权行为的声明。声明应当包括不存在侵权行为的初步证据以及网络用户的真实身份信息。

● 网络服务提供者转声明规则

网络服务提供者接到声明后，应当将该声明转送发出通知的权利人，并告知其可以向有关部门投诉或者向人民法院提起诉讼。网络服务提供者在转送声明到达权利人后的合理期限内，未收到权利人已经投诉或者提起诉讼通知的，应当及时终止所采取的措施。(第一千一百九十六条)

2、加强网络服务提供者的注意义务。网络服务提供者不仅在＂知道”网络用户利用其网络服务侵害他人民事权益时应采取必要措施，并且在“应当知道”此类情形时也应当采取必要措施，否则与该网络用户承担连带责任。(第一千一百九十七条)

四、其他

1、 明确未成年人网络打赏行为效力

未成年人网络打赏行为引发的纠纷颇受社会关注。

《民法典》规定，八周岁以上的未成年人为限制民事行为能力人，实施民事法律行为由其法定代理人代理或者经其法定代理人同意、追认。(第十九条) 不满八周岁的未成年人为无民事行为能力人，由其法定代理人代理实施民事法律行为。(第二十条)

为此，未满八周岁未成年人的网络打赏行为是无效的，监护人可以要求对方返还打赏金额；八周岁以上未成年人的打赏行为需要根据心智成熟状况来区别对待。

2、明确数据和虚拟财产受法律保护

将数据与虚拟财产写入“民事权利”一章，从法律上申明数据、网络虚拟财产受法律保护。(第一百二十七条)

3、完善电子合同订立和履行规则

● 订立

当事人一方通过互联网等信息网络发布的商品或者服务信息符合要约条件的，对方选择该商品或者服务并提交订单成功时合同成立，但是当事人另有约定的除外。(第四百九十一条)

● 履行

通过互联网等信息网络订立的电子合同的标的为交付商品并采用快递物流方式交付的，收货人的签收时间为交付时间。(第五百一十二条)

中科院计算技术研究所大数据研究院

中科院计算技术研究所大数据研究院（简称“数研院”），位于郑东新区龙子湖智慧岛大厦8F，是郑州市政府及郑东新区管委会两级政府全力打造的“产、学、研”结合的新型研发机构，于2018年12月22日在智慧岛正式挂牌。

数研院依托计算所及大数据分析系统国家工程实验室，结合国家大数据（河南）综合试验区的建设需求，开展建设人才培养基地，承担国家重大战略任务，研发自主可控的孵化大数据、云计算、智能制造等创新产业团队的大数据相关工作，构建大数据产业链、价值链、生态链，为“以数据为关键要素”的数字经济提供智力引擎。

数研院构建“一体两翼”的开放格局，打造“政、产、学、研、用”的生态闭环。其中，“一体”为科研，从大数据研究院出发，构建大数据与智能计算创新平台，面向国家战略和推动地方发展的系列研发；“两翼”为产业和教育，通过数研院科研延伸，支撑大数据产业发展和人才培养。