国盟信息安全通报

2020 年 3 月 16 日第 211 期

全国售后服务中心

国盟信息安全通报

（第 211 期）

国际信息安全学习联盟

2020 年 03 月 16 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 554 个，其中高危漏洞 197 个、中危漏洞 271 个、低危漏洞 86 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 33%），其中互联网上出现“Tenda N301 拒绝服务漏洞、Comtrend VR-3033 命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2227 个，与上周（2413 个）环比减少 7%。

主要内容

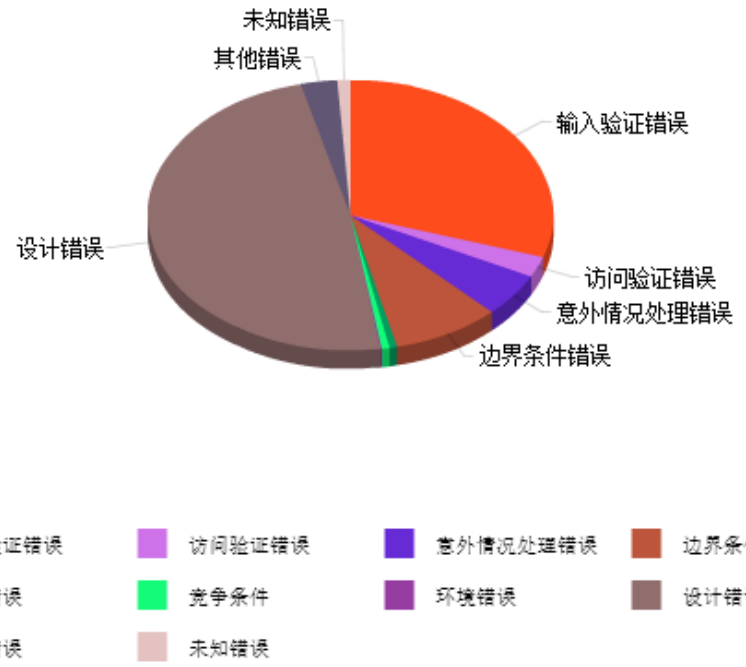
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

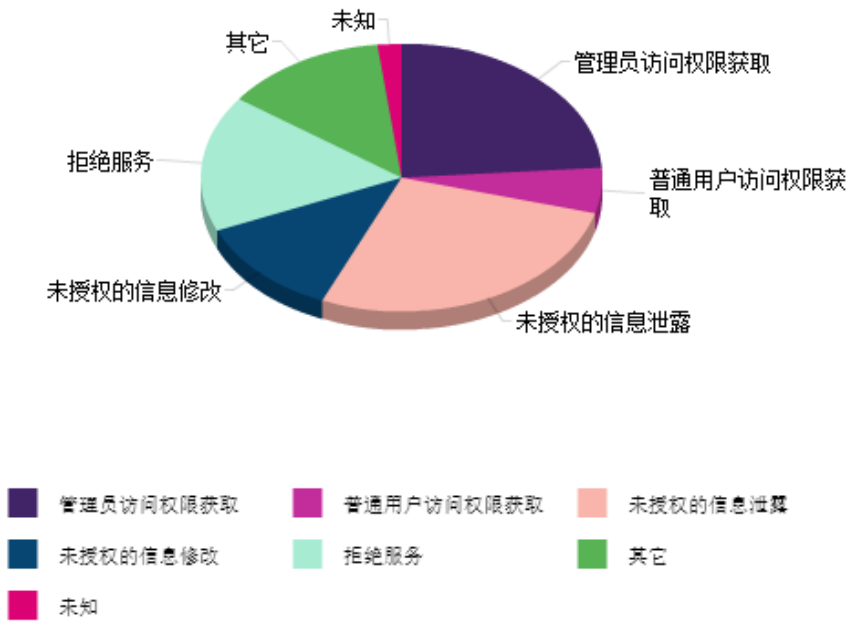
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 554 个，其中高危漏洞 197 个、中危漏洞 271 个、低危漏洞 86 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 33%），其中互联网上出现“Tenda N301 拒绝服务漏洞、Comtrend VR-3033 命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2227 个，与上周（2413 个）环比减少 7%。

二、安全漏洞增长数量及种类分布情况

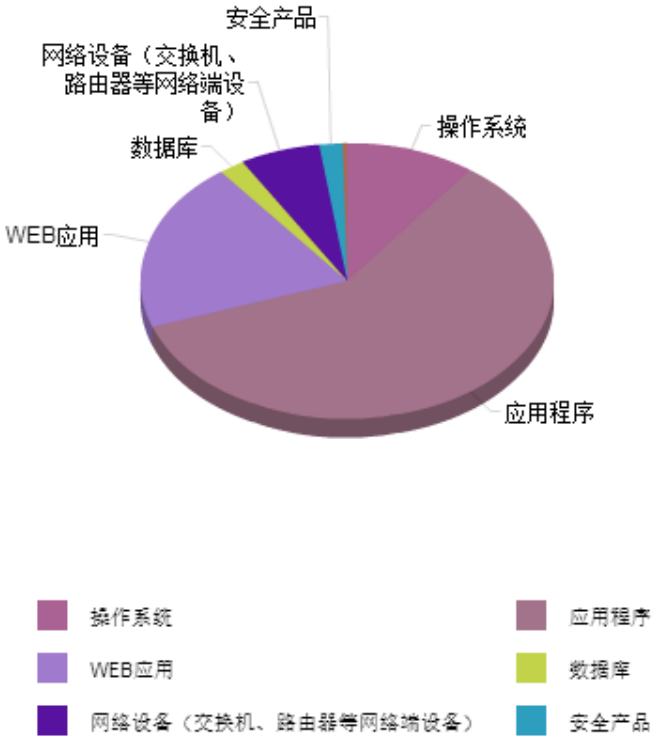
➢ 漏洞产生原因（2020 年 03 月 02 日—2020 年 03 月 15）



➢ 漏洞引发的威胁（2020 年 03 月 02 日—2020 年 03 月 15）



➢ 漏洞影响对象类型（2020 年 03 月 02 日—2020 年 03 月 15）



三、安全产业动态

➢ 我国互联网内容产业现状及发展趋势

随着人工智能、大数据等新技术的广泛应用和全屏生态、粉丝经济、知识付费等新模式的快速兴起，互联网与内容产业融合发展程度日益加深，逐渐发展出不同于传统内容产业的创作传播发展模式，形成互联网内容产业的全新业态。根据载体差异，大致可以分为文图、音频、视频三大类，具体可衍生出网络新闻、网络文学、网络音乐、网络视频、网络直播等多个细分行业。

一、总体发展情况

（一）用户规模持续增长，下沉市场用户加快拓展

随着网络提速降费的推进和智能手机终端的推广，我国网民（尤其是移动网民）数量迅速攀升，据 CNNIC 统计信息显示，截至 2019 年 6 月，我国网民规模已达 8.54 亿，其中手机网民规模达 8.47 亿，人口渗透率超 60%。数量庞大的中国网民和便捷低价的互联网接入服务为互联网内容产业的繁荣发展奠定了坚实的基础。从用户数量上来看，截至 2019 年 6 月，我国网络新闻、网络文学、网络音乐、网络视频、网络直播的用户数量分别达 6.86 亿、4.55 亿、6.08 亿、7.59 亿和 4.33 亿，分别较 2018 年底增长 1.7%、5.2%、5.6%、4.7%和 9.2%。从行业布局来看，网络新闻和网络视频用户已取得较好开发，网民渗透率分别达到 80.3%和 88.9%，一二线城市用户基本已被龙头企业瓜分完毕，用户增量空间有限，部分以下沉市场

为目标的企业获得快速增长，如趣头条 2019 年一季度,装机用户数已突破 4 亿,月活跃用户数达 1.1 亿,其中来自三线及以下城市用户占比超过七成。

（二）内容生产门槛降低，行业社交属性突显

随着在线内容创作工具和内容分享平台的完善和发展，内容创作的成本和门槛进一步降低，大批潜在创作者被激活，积极依托自身资源输出信息。用户不再是信息的被动消费者，而是成为内容创作的深度参与者，图文社区、短视频社区等深度互动模式迅速兴起，互联网内容产业由早期的人与作品互动逐渐演变为人与人的互动，内容的社交属性日益强化。如抖音等短视频平台通过降低视频制作难度、内置多样拍摄模式、引导用户参与高热度话题等方式迅速积聚大量用户，成为新兴流量入口。

（三）信息流成推送主流，内容质量成竞争重点

信息流是指在一屏界面中展示连续的定制内容，具有强个性化、高信息密度的显著特征，操作便捷且能迅速提供有效内容，利于唤起用户情绪和提升用户使用时长，逐渐成为今日头条、抖音、知乎等 App 的主要推送手段。随着信息流的广泛应用，用户时刻处于高频率、高强度的内容推送中，大量冗余、低质内容堆积，信息流模式本身能提供的用户和使用时长增长已经非常有限，推送的内容本身才是关键。部分平台大力鼓励原创、积极引入优质内容团队，大力提升了内容输出的稳定性和专业性，如知乎发展优质大 v、抖音积极引入官方机构入驻等。部分平台瞄准细分领域，打造垂直型内容生态，如主打财经资讯的“功夫财经”、主打家庭美食的“日日煮”，以及美妆类短视频应用“小红唇”等。部分平台积极发展自制内容吸引用户，如爱奇艺的自制综艺偶像练习生、自制古装剧延禧攻略，腾讯视频自制综艺创造 101，得到的听书音频等。

(四)知识产权保护力度加大，内容付费模式兴起

近年来我国加大知识产权保护力度，连续多年开展网络侵权盗版的“剑网行动”，全社会版权意识上升，用户为优质内容、优质服务的付费意识日益强烈。随着大量专业性、差异化优质内容涌现，内容付费快速崛起，成为继广告、电商之后内容平台变现的重要模式。2018 年中国网络版权产业市场规模达 7423 亿元，同比增长 16.6%，其中用户付费规模接近 3686 亿元，同比增长 15.8%。内容付费方式主要有为优质作品付费和为优质服务付费两类。为优质作品付费主要包括购买电子书、音频、视频课程、在线电影等作品，以及文章打赏、在线问答等形式；付为优质服务付费费主要包括购买会员等。

二、行业发展趋势

（一）监管日益完善，行业走向合规发展

互联网内容产业发展中存在的问题逐渐暴露，如创作者为了吸引眼球生产违背公序良俗的低俗内容，内容平台审核不力公然传播不良信息，盗版、抄袭、洗稿等版权侵权手段层出不穷，个人信息保护不力，巨头企业流量劫持、屏蔽对手的不正当竞争行为等。随着监管力度的加大，内容审核、版权保护、个人信息保护、规范竞争等方面的合规化进程加快，互联网内容产业将逐渐脱离野蛮增长进入健康经营。

（二）用户与流量向头部集中，马太效应凸显

支撑内容创作和传播新媒体、直播、短视频等模式兴起后，大量新内容涌入，颠覆原有的用户流量集聚中心，内容生产去中心化。但随着新模式的成熟，早布局、发展快的企业凭借用户基础、资本实力和产业链布局能力形成新的中心，聚集大量优质 IP 和 KOL，购入和自制大量优质内容，成为头部企业，收获大部分用户和流量，直至新模式带来颠覆。

（三）持续技术和业务创新，积极开拓新市场

互联网内容领域创新活跃、迭代迅速，未来可能的创新方向有四：一是通过传播途径创新激活低付费意愿的用户群体，如社交裂变等。二是通过运营方式创新提升用户价值，将信息流与内容变现更深度融合。三是通过模式创新直击用户痛点，锁定空白产品与服务市场获得新机遇。四是通过新技术应用带来内容载体和传播模式的变化，如 5G 时代可能取得发展的 VR/AR、互动剧集等。

三、政策建议

互联网内容产业仍处于快速发展过程中，新技术、新模式、新业态持续涌现，在推动产业合规和升级发展的过程中，行业监管起着重要的引路人作用，需平衡好加强监管和鼓励创新之间的关系。一方面，在促进产业繁荣的过程中，需要划清底线，不断完善产权保护、信息保护、内容审核的法制法规，加强事中事后监管，营造良好发展环境。另一方面，在推进产业合规的进程中，需保持政策的连贯和稳定性，不搞一刀切和断崖式管理，畅通与企业、创作者、消费者之间的沟通途径，降低行业创新风险。（来源：中国信通院）

➢ 阻击疫情，不能冲击个人信息安全防线

随着新型冠状病毒感染的肺炎疫情的蔓延，各个省份和地区的防控措施逐步升级。为了更好地做好疫情防控工作，全国各地都对武汉返乡人员进行了信息登记，这些信息精确到姓名、身份证号码、户籍地址、家庭住址、手机号码等等。

然而，一些政府部门统计的信息本来是为了实时监控、掌握情况，而今，却变成了一张张公开被线上追杀的“通缉令”。

各地武汉返乡人员的名单开始在各种家人群、同学群中疯传，个人隐私信息一应俱全。个别被公开信息的人员还受到了陌生人电话、微信等方式的骚扰，其中也不乏信息不实现象。一时间，武汉返乡人员信息遭泄露登上了热搜。疫情之下，暴露出人们对信息尽可能详尽公开的渴望，但同时，无底线地泄露个人信息则涉嫌侵犯个人隐私。那么，个人信息该如何公开，才能既阻击疫情又不侵犯个人隐私?

信息详细公开 利于精准防控疫情

毕竟，乘客的性别、年龄、返乡日期、活动区间这些内容，一方面有助于加强对新型冠状病毒及其发展情况的了解;另一方面也能提醒市民防范，利于疫情防控。

中国医师协会法律事务部主任邓利强说，按照传染病防治法的疫情报告规定，“只发布什么病有多少例，这些最基本的信息，满足了法律对行政机关的最低要求。”

但是在突发公共卫生事件或者传染病暴发、流行的时候，这些最基本的信息是不是能够满足公众的知情权?邓利强直言，答案是否定的。

邓利强表示，地方政府公布疫情信息首先必须发布应该发布的信息，就是传染病传播的基本信息;第二，如果不侵犯到个人隐私权，“在当前情形下，越详细越好，天花板是个人的隐私权。”

“我国多地已经启动公共卫生事件一级响应，已经说明了此次事件的紧急性和严重性，在涉及重大公共利益的情形下，公民个人的隐私权应当进行克减。”上海社会科学院法学研究所研究员彭峰说。

华中科技大学同济医学院公共卫生学院教授吴志刚认为，地方政府发布疫情信息主要有两个考量：既要让社会大众知道危害性，让人民群众有自觉防范的意识，又要保障社会正常秩序。”

不过，究竟需要多大程度地公开?

“应对疫情和保护隐私，确实是硬币两面，处理好这对矛盾的关键，就在于信息公布要拿捏好分寸。”罗志华医生认为，公布确诊病例所在小区信息，在宏观上不仅利于做到精准防控，具体到小区个人，也能提高自我防护意识。只要拿捏好信息公布的分寸，以及协调好相关配套措施，公布相关病例涉及小区及场所，在抗疫的特殊时期有其推广价值。他分析，过于抽象模糊不利于防疫，过于具体则不利于保护患者，将确诊病例的位置信息公布到小区这一级，在应对疫情和保护隐私两方面都得以兼顾。

信息过度泄露 涉嫌侵犯个人隐私

通过各地已发生和正在发生，歧视或者骚扰武汉归乡人员的事件可以看出，身份证号码、手机号码等信息不但未能有效服务公众利益，还严重侵犯了个人隐私权。

网络完全法第四十四条规定，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。同时，传染病防治法第十二条规定：“疾病预防控制机构、医疗机构不得泄露涉及个人隐私的有关信息、资料。”

据央视报道，App 专项治理工作组的专家说，没有明确法律授权的组织和机构，或者不是依法参与政府组织开展疫情防控工作的人员，不得未经被收集者同意而收集使用确诊者、疑似者及密切接触者的个人信息，更不能在微信群、朋友圈等私自传播上述信息，否则属于侵害公民个人信息的行为，情节严重的可能构成侵害公民个人信息罪。如果是疾病预防控制机构、医疗机构、基层工作人员等泄露上述信息，还会构成加重情节。

同时，App 专项治理工作组的专家表示，结合当前疫情防控背景和民众的恐慌情绪影响，肺炎确诊者、疑似者及密切接触者往往被视为高危人群，其个人信息一旦泄露、传播可能会引发一些骚扰、恐吓行为，甚至出现已被确诊的谣言等等，这可能会使得信息被公开人员及其家人的身心健康受到损害或者引发歧视性待遇等，这些信息理应作为个人敏感信息受到更高程度的保护。

太琨律创始合伙人朱界平律师分析：现代社会，个人信息保护被置于非常重要的地位，我国法律体系中对于个人信息安全保护的相关法律规定也在逐渐完善，现行的网络安全法、民法总则、治安管理处罚法、消费者权益保护法等法律均对个人信息保护作了相关的规定。他指出，在刑事方面，我国刑法第二百五十三条规定了侵犯公民个人信息罪，对于侵犯公民个人信息构成犯罪的，依法追究刑事责任。

朱界平认为，基于当前疫情防控形式，对于个人信息的适度公开，能更好地保护大多数人的生命和健康权利益，应优先于个人信息的保护。

精准联防联控 做好个人信息保护

在战“疫”的重要阶段，不论是相关部门还是个人，都需要掌握好知情权与隐私权的平衡，拿捏好分寸，避免造成次生伤害。

1 月 30 日，交通运输部发布紧急通知，要求依法严格保护个人隐私和个人信息安全，除因疫情防控需要，向卫生健康等部门提供乘客信息外，不得向其他机构、组织或者个人泄露有关信息、不得擅自在互联网散播。

2 月 9 日，中央网信办公开发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，通知明确了为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

对于有关组织对外披露疫情相关的信息时，如何平衡信息公开及个人信息保护呢?App 专项治理工作组的专家认为，对于疫情报告、通报和公布等对外披露工作，仅公开返乡人员流动统计数据、确诊患者仅公开性别、确诊日期、发病症状等非个人信息，即可满足社会一般公众对疫情状况的知情权，而不应公开姓名、年龄、身份证号码、电话号码、家庭住址等。对于确诊或疑似病例所在地区的公众，可公开确诊或疑似病例的大致居住区域，满足此类公众对防控需求的知情权，不必要公开其具体的个人信息。

上海交大数据法律研究中心执行主任何渊认为，我们必须在维护公民知情权、数据利用与社会整体性利益之间实现平衡。面对来势汹汹的新型冠状病毒，我们必须把握好政府信息公开及数据开放的法律边界及“颗粒度”，即不得突破“三安全一稳定(国家安全、公共安全、经济安全及社会稳定)”及“二秘密一隐私(国家秘密、商业秘密及个人隐私)”等底线思维。

在这场战“疫”中，我们既要积极利用包括个人信息在内的大数据支撑联防联控工作，更要守住个人信息保护底线。（来源：法制网）

➢ 深度解读《网络信息内容生态治理规定》

为了营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益，构建天朗气清的网络空间，国家互联网信息办公室于 2019 年 12 月 15 日发布《网络信息内容生态治理规定》（以下称：《治理规定》），自 2020 年 3 月 1 日起正式施行。

《治理规定》集中体现了习近平总书记关于“网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益”的重要指示精神，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，突出了“政府、企业、社会、网民”等多元主体参与网络生态治理的主观能动性，重点规范网络信息内容生产者、网络信息内容服务平台、网络信息内容服务使用者以及网络行业组织在网络生态治理中的权利与义务，这是我国网络信息内容生态治理法治领域的一项里程碑事件，而且以“网络信息内容生态”作为网络空间治理立法的目标，这在全球也属首创。

一、网络信息内容生态治理符合“以人民为中心”的理念

生态（Eco-）一词源于古希腊字，意思是指人类的家园或者人类生存的环境。习近平总书记在“4·19”讲话中指出，网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。谁都不愿生活在一个充斥着虚假、诈骗、攻击、谩骂、恐怖、色情、暴力的空间。

《治理规定》将“网络信息内容生态治理”定义为，政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

上述定义反映了党的十九届四中全会《决定》中提出的“建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间”的精神，特别是集中体现了习近平总书记关于“国家网络安全工作要

坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益”的重要思想，符合“以人民为中心”的发展理念，为我国建立网络综合治理体系奠定了坚实的法治基础。

二、《治理规定》突出了网络信息内容生态治理主体的多元化

网络信息内容生态的治理，应当明确多元参与协同共治的治理模式，要突破市场和政府二元对立和单一主导的模式。在数字经济时代，要以平台思维和社会化思维的模式重新审视政府、企业、社会、网民这四大主体在网络生态治理中的功能和作用。他们已经不是主体支配和被支配的关系，而是基于共同利益和目标的伙伴式关系。

《治理规定》明确了政府、企业、社会、网民等主体多元参与协同共治的治理模式。事实上，网络信息内容生态是由多种文明要素组成的系统，这些要素主要包括网络主体、网络信息、主体行为、技术应用、基础设施保障、网络政策法规和网络文化等方面。笔者认为，在参与网络生态治理的四大主体中，政府的作用是监管、企业的义务是履责、社会的功能是监督、网民的义务是自律。

首先，国家网信部门负责统筹协调全国网络信息内容生态治理和相关监督管理工作，各有关主管部门依据各自职责做好网络信息内容生态治理工作；

其次，网络信息内容生产者，是制作、复制、发布网络信息内容的组织或者个人，应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益，特别是网络信息内容服务平台企业应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化；

再次，充分发挥网络监督作为网络信息内容的重要监督方式，这是发挥社会监督最有效、最简单、最直接的形式，能够形成在网络信息内容治理领域，人人皆监督、人人受监督的局面；

第四，网络时代使人类进入到一个无限内容生产的时代，人人都是内容生产者。因此，网络信息内容的治理更多的是以网民自律的形式对自身行为的规范和矫正，这是网络信息内容生态治理一个极其重要的方面。

三、《治理规定》重点规制三大管理相对人

在网络信息内容生态治理行政法律关系中，与行政主体相对应一方的公民、法人和其他组织是网络生态治理的行政管理相对人。鉴于网络生态治理的对象是网络信息内容，而信息内容的生态治理主要涉及三类主体，即内容的生产者、内容的服务平台和内容服务的使用者，为此《治理规定》重点规制这三大行政管理相对人。

首先，网络信息内容生产者，是制作、复制、发布网络信息内容的组织或者个人，作为制作网络信息内容的组织或者个人，在遵守法律法规的前提下，还要遵循公序良俗，加强网络文明建设；不得制作、复制、发布《治理规定》禁止的违法信息内容，并采取一系列措施，防范和抵制制作、复制、发布《治理规定》明确的不良信息内容；

其次，网络信息内容服务平台，是提供网络信息内容传播服务的网络信息服务提供者，应当重点建立网络信息内容生态治理机制，一是制定本平台网络信息内容生态治理细则；二是健全平台管理制度，重点应当建立和完善用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度；

再次，网络信息内容服务使用者，是使用网络信息内容服务的组织或者个人，这是网络生态治理的主力军，应当严守两条底线，一是应当以文明健康的方式使用网络，按照法律法规的要求和用户协议约定，切实履行相应的法律义务；二是在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布违法信息，防范和抵制《治理规定》明确的不良信息。同时，对网上的违法和不良信息内容有义务以投诉、举报等方式行使监督权。

《治理规定》明确了网络群组、论坛社区版块的建立者和管理者应当履行管理责任，依法依约规范群组、版块内信息发布等行为；《治理规定》明确要求，网络信息内容服务使用者和生产者、平台不得开展网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等违法活动。

四、网络信息内容生产者禁止触碰的十条红线

当前，移动互联网应用程序（App）已成为移动互联网信息服务生产的主要载体，对提供民生服务和促进经济社会发展发挥了一定的作用，与此同时，少数 App 也被不法分子利用，传播暴力恐怖、淫秽色情及谣言等违法违规信息，有的存在窃取隐私、恶意扣费、诱骗欺诈等损害用户合法权益的行为，多数 App 过度收集个人信息，且设置的所谓“隐私条款”侵犯用户个人信息权，社会反映强烈。

我国网络信息内容生产者数量庞大，截至 2019 年 12 月，我国国内市场上监测到的 App 数量为 367 万款，第三方应用商店在架应用分发总量达到 9502 亿次，其中社交通讯类下载量达 1166 亿次。据腾讯发布的数据显示，2019 年仅微信的月活跃账户数超过了 11.5 亿，QQ 的整体月活跃账户数增至 8.23 亿，每天有近 450 多亿条消息在微信里传输。

习近平总书记强调，利用网络鼓吹推翻国家政权，煽动宗教极端主义，宣扬民族分裂思想，教唆暴力恐怖活动等等，这样的行为要坚决制止和打击，决不能任其大行其道；利用网

络进行欺诈活动，散布色情材料，进行人身攻击，兜售非法物品等等，这样的言行也要坚决管控，决不能任其大行其道。没有哪个国家会允许这样的行为泛滥开来。对此，《治理规定》第六条明确了网络信息内容生产者禁止触碰的十条红线：

一是反对宪法所确定的基本原则的；二是危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；三是损害国家荣誉和利益的；四是歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；五是宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；六是煽动民族仇恨、民族歧视，破坏民族团结的；七是破坏国家宗教政策，宣扬邪教和封建迷信的；八是散布谣言，扰乱经济秩序和社会秩序的；九是散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；十是侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的。

网络信息内容生产者违反上述规定，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。

五、网络信息内容生产者应当防范和抵制八类不良信息

《治理规定》要求网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列八类内容的不良信息：

1.使用夸张标题，内容与标题严重不符的信息内容。“标题党“是互联网上利用各种颇具创意的标题吸引网友眼球，以达到各种目的，其主要行为简而言之即发帖的标题严重夸张，帖子内容通常与标题完全无关或联系不大，诸如震惊、惊爆、重磅、罕见、深度好文、轰动全国、绝密偷拍等字眼。笔者在网上搜索了类似“震惊 13 亿中国人“、“感动了中国 13 亿人“、”重磅“、”深度好文“等标题，其内容与标题完全不符，多数以夸张的、曲解的、煽情的甚至无中生有的方式误导网民。

2.炒作绯闻、丑闻、劣迹等信息内容。当前，娱乐界炒作绯闻、丑闻以及劣迹比比皆是，以明星绯闻八卦为噱头，特别是通过明星和狗仔队的配合来制造绯闻、丑闻、劣迹的热度，这些低俗文化和行为愚弄了大众、污染了网络、触碰了法律，必须依法治理。

3.不当评述自然灾害、重大事故等灾难的信息内容。我国地域广、人口密集，自然灾害种类多，重大安全事故时有发生。笔者注意到，每当自然灾害和重大安全事故等灾难发生时，总有一些没有事实依据的评述，不仅混淆了是非，而且给社会带来极大的负面影响，必须坚决予以抵制。

4.带有性暗示、性挑逗等易使人产生性联想的信息内容。为了吸引流量，一些网络平台，

以文字、语音、图片、视频等方式进行带有“性挑逗”、“性暗示“的不良行为，比如所谓的“文爱”、“磕炮”等，这些信息内容均带有性暗示或性挑逗的软色情内容，极容易使人产生性联想。

我国《刑法》对淫秽物品的定义是，具体描绘性行为或者露骨宣扬色情的诲淫性的书刊、影片、录像、图片等，但是将有关人体生理、医学知识的科学著作和包含有色情内容的有艺术价值的文学、艺术作品排除在淫秽物品范围之外。

5.展现血腥、惊悚、残忍等致人身心不适的信息内容。一些网络内容制作者为了骗取用户的点击量，发布和展示血腥、惊悚、残忍的图片和视频，如有的网站发布大量令人不适的惊悚、血腥、虐杀动物、畸形胎儿的图片，同时还兼有“标题党”嫌疑，致人身心感到极大地不适，尤其是对未成年的心理损害极其严重。

6.煽动人群歧视、地域歧视等的信息内容。煽动是指怂恿、鼓动人做坏事的行为，我们经常在网上看到，一些人仅凭自己看到的只言片语就在网上传播并发布地域歧视和人群歧视等过激言论。如有一则“医院多次医疗事故不能给公众解释”的网络帖子，煽动当地人群对医生群体的歧视，该发布者因涉嫌寻衅滋事被公安机关行政拘留 10 日。

7.宣扬低俗、庸俗、媚俗内容的信息内容。主要是两类信息内容，一是低俗的内容，主要是指低级趣味、庸俗，使人萎靡、颓废的内容；二是媚俗的信息内容，主要是那些迎合于世俗，缺乏自我思想、自我理智，只知随波逐流等，这些低俗、庸俗、媚俗的信息内容与我国优秀道德文化和时代精神格格不入，必须坚决抵制。

8.可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的信息内容。当前，我国未成年人网民数量近 1.7 亿，智能手机成为未成年人上网的主要工具，未成年人正处于青春躁动期，有很强的求知欲望，他们对网络发布的一些不安全和违反公德的信息内容鉴别力很弱、自控能力较差，很容易在模仿后导致恶性事件的发生，未成年人模仿网络不良行为已经成为威胁青少年网络安全的主要因素。

六、三大管理相对人的共同禁止性行为

《治理规定》要求网络信息内容服务使用者、网络信息内容生产者和网络信息内容服务平台共同营造良好网络生态，不得实施以下禁止性规定。

1.不得利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私等违法行为，损害他人合法权。行为人利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私，是严重的侵权行为，这不仅涉及网络信息内容生产者，也涉及网络信息内容服务使用者和网络信息内容服务平台。

根据《侵权责任法》的规定，网络用户利用网络服务实施侵权行为的，被侵权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。网络服务提供者接到通知后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。如果网络服务提供者知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。

2.不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益。笔者认为，应当重点治理网络信息内容服务平台为了谋取不正当利益通过发布、转载、删除信息以及干预信息内容呈现或搜索结果等违法行为。

3.不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。AI 的深度学习在搜索技术、数据挖掘、机器学习、机器翻译、自然语言处理、多媒体学习等领域应用广泛；虚拟现实（VR）是一种灵境技术，其基本实现方式是计算机模拟虚拟环境从而给人以环境沉浸感。无论是深度学习，还是 VR 技术均与信息内容有直接关联，利用这些技术应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益。

4.不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。

近年来，App 刷量、电商刷单、公号刷阅读量等网络的黑色产业屡遭曝光，一些互联网应用平台通过技术手段篡改、诱导等违规方式将他人的用户导向自己的产品或服务，实施流量劫持，获取不正当商业利益的行为。笔者注意到，很多网络违法和黑色交易，都与虚假注册账号、非法交易账号、操纵用户账号等行为有关联，这已经形成黑色产业链，通过虚假注册账号、非法交易账号、操纵用户账号，能获得大量账号资源，为不法行为提供网络身份，以此隐蔽真实身份，制造虚假流量，增加溯源难度，逃避法律追究。

5.不得利用党旗、党徽、国旗、国徽、国歌等代表党和国家形象的标识及内容，或者借国家重大活动、重大纪念日和国家机关及其工作人员名义等，违法违规开展网络商业营销活动。

中国共产党的党徽党旗是中国共产党的象征和标志，根据《中国共产党党章》的规定，党的各级组织和每一个党员都要维护党徽党旗的尊严，要按照规定制作和使用党徽党旗；国徽和国歌是《宪法》规定的国家形象标识和内容，任何商业组织都不得用于商业营销活动。

七、网络信息内容生态治理的监督机制

《治理规定》要求各级网信部门会同有关主管部门，建立健全信息共享、会商通报、联合执法、案件督办、信息公开等工作机制，协同开展网络信息内容生态治理工作。事实上，

我国网络信息内容治理的监管不仅仅是网信部门的职责，应当全面把握网络综合治理体系的各个要素和环节，增强协同体系监管的顶层设计。

对网络信息内容的监管，重点是对网络信息内容服务平台履行信息内容管理主体责任情况的监管，特别是要针对自媒体的无序和乱象，平台企业负有不可推卸的责任。应当指出，信息内容平台企业不仅是自媒体运营的服务提供者，也是自媒体行业秩序的维护者，必须履行好责任义务，依法运营，严格履行信息内容管理的主体责任。

《治理规定》要求，各级网信部门建立网络信息内容服务平台违法违规行为台账管理制度，并依法依规进行相应处理。笔者认为，网络信息内容服务平台违法违规行为台账管理制度，是对平台企业的一项重要管理制度，反映和记载了平台内各类信息内容违法违规的行为和内容以及分布区域和数量的动态情况等，为网络主管机构实施信息内容监管提供了有力的事实和证据。

整体上看，《治理规定》体现了国家在网络信息内容生态治理领域的主权价值取向，展示了网络空间的自由和秩序、开放和自主、管理和服务的辩证关系，重点突出了网络信息内容生态治理的统筹与协调，随着《治理规定》的正式实施，我国网络信息内容的生态治理将正式纳入法治轨道，并将依法形成治理合力。（来源：“网信中国”）

➢ 最新《个人信息安全规范》正式稿九大主要变化两大焦点问题解读

2020 年 3 月 7 日消息，根据 2020 年 3 月 6 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 1 号），全国信息安全标准化技术委员会（以下简称“信安标委”）归口的 GB/T 35273-2020《信息安全技术 个人信息安全规范》以下简称“《规范》（2020 正式稿）”）等 8 项国家标准正式发布，将于 2020 年 10 月 1 日正式实施。

作为个人信息安全领域最基础、最重要和影响最为广泛的国家标准，《个人信息安全规范》（2020 正式稿）的发布和实施，对后续个人信息保护工作的开展将会产生深远影响。接下来，将首先通过与《规范（征求意见稿）》（2019.10.22 版）对比的方式，为大家梳理解读《规范》（2020 正式稿）的九大主要变化，方便大家快速了解掌握重点内容。其次，对于大家最关心的《规范》（2020 正式稿）的修改历程和效力问题，我们也进行了整理。最后，文末附上了《规范（征求意见稿）》（2019.10.22 版）和《规范》（2020 正式稿）逐条对比表格

的获取方式，供大家参考。

九大主要变化速览

序号	主要变化
1.	删减收集个人信息合法性的部分要求
2.	新增及强化个人生物识别信息的收集、存储和共享转让的要求
3.	新增采用密码技术宜遵循密码管理相关国家标准的要求
4.	将“隐私政策”调整为“个人信息保护政策”
5.	将个人信息主体的权利作为专门的条款要求
6.	优化个人信息主体注销账户的相关规定
7.	放宽第三方接入管理的部分要求
8.	放宽任命专职个人信息保护负责人和个人信息保护工作机构的部分条件
9.	新增建立自动化审计系统的要求

企业最关心的两大问题目录

序号	主要变化
1	《个人信息安全规范》GB/T 35273-2020 的修订历程
2	《个人信息安全规范》GB/T 35273-2020 的效力

第一部分、九大主要变化具体解析

主要变化一：删减收集个人信息合法性的部分要求

【条文对比】

《规范（征求意见稿）》（2019.10.22 版）	《规范》（2020 正式稿）
5.1 收集个人信息的合法性 对个人信息控制者的要求包括： a) 不应以欺诈、诱骗、误导的方式收集个人信息； b) 不应隐瞒产品或服务所具有的收集个人信息的业务功能； c) 不应从非法渠道获取个人信息； ~~d) 不应收集法律法规明令禁止收集的个人信息；~~ ~~e) 不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人敏感信息。~~	5.1 收集个人信息的合法性 对个人信息控制者的要求包括： a) 不应以欺诈、诱骗、误导的方式收集个人信息； b) 不应隐瞒产品或服务所具有的收集个人信息的功能； c) 不应从非法渠道获取个人信息。

【解读】：根据条文对比，可以看出，对于收集个人信息的合法性要求，《规范》（2020 正式稿）删除了原有的“不应收集法律法规明令禁止收集的个人信息”和“不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人敏感信息”的要求。

1、删除“不应收集法律法规明令禁止收集的个人信息”的要求

对于删除“不应收集法律法规明令禁止收集的个人信息”的要求，如法律法规已经明令禁止收集某类个人信息，个人信息控制者本就应该遵循相应法律法规的规定。以征信业务为例，《征信业管理条例》第十四条明确规定，禁止征信机构采集个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。也就是说，行政法规明确禁止征信机构在征信业务中收集前述个人信息。

2、删除“不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人信息”的要求

对于删除“不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人信息”的要求，意味着，从字面意思理解，个人信息控制者可以大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人信息。但需要指出的是，Facebook 数据泄露事件为全世界敲响了警钟，大规模收集我国公民的前述信息，一旦泄露或被不法分子加以非法利用，很容易给我国国家安全、社会稳定和民族团结造成严重威胁。建议企业从实际业务需求出发，在确为业务开展所必需的情况下，方可大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人信息。如收集该等信息，应加强对该等个人信息的安全保护，尽可能防止其被窃取、泄露或其他个人信息安全事件的发生，以减少对我国国家安全、社会稳定和民族团结的潜在威胁。

此外，需要指出的是，《规范》（2020 正式稿）保留了不应公开披露前述信息分析结果的要求，即第 9.4g)条要求“不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果”。这就意味着，企业可以收集我国公民的种族、民族、政治观点、宗教信仰等个人信息，但不应将该等信息的分析结果进行公开披露，其目的主要也是在于减少对我国国家安全、社会稳定和民族团结的潜在威胁。

主要变化二：新增及强化个人生物识别信息的收集、存储和共享转让的要求

【条文对比一】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
无	5.4 收集个人信息时的授权同意 …… c) 收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。 注 3：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面都识别特征等。

【解读】:《规范》（2020 正式稿）新增了对收集个人生物识别信息的要求。

在探讨对收集个人生物识别信息的要求前，我们需要先来探讨一个问题，为什么要新增对个人生物识别信息的强化保护？《信息技术 安全技术 生物特征识别信息的保护要求（征求意见稿）》在其引言部分指出了个人生物识别信息需要加以保护的原因。简单来说，一方面，个人生物识别信息用于身份鉴别有其独特优势，比如手机指纹解锁、人脸解锁、人脸支付、声音锁等。因为一般来说个人生物识别信息难以或不可能发生变化、与个人密切绑定且不同人的信息不一致；但另一方面，也正因为个人生物识别信息难以或不可能发生变化、与个人密切绑定，其一旦出现被泄漏、被窃取等安全事件，通常的更改密码、发新令牌等身份鉴别更新措施都难以奏效，也很容易给个人信息主体造成财产损失、名誉损失等严重后果。之前出现的小学生用照片刷开了某智能快递柜、换脸软件“ZAO”引发的对刷脸支付安全性的担忧，都与个人生物识别信息的应用直接相关。基于此，需要对个人生物识别信息进行强化保护。

对于收集个人生物识别信息的要求看，包括告知方式、告知内容和同意方式三个要点：

（1）告知方式，单独告知；

（2）告知内容，收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则；

（3）同意方式，明示同意。

从理解适用角度，只将个人生物识别信息的相关规则放置在个人信息保护政策中，可能

已经无法满足《规范》（2020 正式稿）的要求。可供参考的模式为，企业对个人生物识别信息制定单独的个人生物识别信息保护政策或个人生物识别信息保护说明，在实际开始采集个人生物信息前弹窗告知个人生物识别信息保护的简要规则并放置完整版个人生物识别信息保护政策或个人生物识别信息保护说明的链接，通过用户手动点击确认弹窗内容来获得用户的明示同意。但是否确切能够满足《规范》（2020 正式版）的要求，还有待实践的进一步探索和监管部门的进一步意见。

【条文对比二】

《规范（征求意见稿）》（2019.10.22 版）	《规范》（2020 正式稿）
6.3 个人敏感信息的传输和存储 b) 存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅收集、存储、使用摘要信息。	6.3 个人敏感信息的传输和存储 b) 个人生物识别信息应与个人身份信息分开存储； c) 原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于： 1) 仅存储个人生物识别信息的摘要信息； 2) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能； 3) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。 注 2：摘要信息通常具有不可逆特点，无法回溯到原始信息。 注 3：个人信息控制者履行法律法规规定的义务相关的情形除外。

【解读】:《规范》（2020 正式稿）对存储个人生物识别信息，提出了较《规范（征求意见稿）》（2019.10.22 版）更为严格的要求。

《规范》（2020 正式稿）明确了原则上不应存储原始个人生物识别信息（如样本、图像等）的要求。这意味着，不存储原始个人生物识别信息是原则要求，一般来说不得突破该要求。如果想要存储原始个人生物识别信息，需要有特别充分的依据。什么能够算是特别充分的依据？注 3 给出了一种依据，个人信息控制者履行法律法规规定的义务相关的情形除外，也就是说为了履行法律法规规定的义务可以存储原始个人生物识别信息，这个适用条件可以

说已经很严苛了。

《规范》（2020 正式稿）对存储个人生物识别信息提供了更多的路径参考。第一条可选路径，在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能，意味着个人生物识别信息存储在用户的手机等采集终端，身份识别、认证等动作在用户的手机等终端上完成，而不需要将个人生物识别信息传送至企业，企业接收的只是该等信息验证的结果。比如，支付宝在其《隐私政策》（2019.12.11 生效版本）中列明“您需在您的设备上录入您的指纹信息或面容 ID 信息，在您进行指纹支付或面容 ID 支付时，您需在您的设备上完成信息验证。我们仅接收验证结果，并不收集您的指纹信息或面容 ID 信息。”第二条可选路径，在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。意味着采集了个人生物识别信息的原始图像用于识别身份、认证等，但用完就删除原始图像，简单来说就是采集以后用了，用完就删除了。从删除时间来说，宜在用完个人信息后立即删除。

《规范》（2020 正式稿）强调了个人生物识别信息摘要信息的不可逆性，即要求无法自摘要信息回溯到原始信息。如果摘要信息能够回溯到个人生物识别信息的原始信息，摘要的意义将不复存在，也是对不应存储原始个人生物识别信息（如样本、图像等）的原则要求的规避。

【条文对比三】

《规范（征求意见稿）》（2019.10.22 版）	《规范》（2020 正式稿）
无	9.2 个人信息共享、转让 i) 个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

【解读】:《规范》（2020 正式版）新增了对个人生物识别信息共享、转让的要求。

从要求看，不共享、转让个人生物识别信息为原则，确需共享、转让需符合以下四个条件要求：（1）必要性，确因业务需要。也就意味着，共享转让个人生物识别信息需要经得起必要性的检验，在面临监管检查和公众质疑时需要有足够的业务需要作为支撑；（2）告知方

式，单独告知；（3）告知内容，告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等；（4）同意方式，明示同意。

从理解适用角度，可供参考的模式为，如确需对外共享、转让个人生物识别信息的，在个人生物识别信息保护规则或说明中告知用户前述需要告知的内容，并通过征得用户对个人生物识别信息规则的明示同意的方式，来满足这里对于共享、转让个人生物识别信息的明示同意要求。但是否确切能够满足《规范》（2020 正式版）的要求，还有待实践的进一步探索和监管部门的进一步意见。

主要变化三：新增采用密码技术宜遵循密码管理相关国家标准的要求

【条文对比】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
6.3 个人敏感信息的传输和存储 对个人信息控制者的要求包括： a) 传输和存储个人敏感信息时，应采用加密等安全措施； ……	6.3 个人敏感信息的传输和存储 对个人信息控制者的要求包括： a) 传输和存储个人敏感信息时，应采用加密等安全措施； 注：采用密码技术时宜遵循密码管理相关国家标准。 ……

【解读】：《规范》（2020 正式版）新增采用密码技术宜遵循密码管理相关国家标准的要求，按照该等国家标准执行有助于规范密码技术的使用、提高密码的防护能力，更好地保障个人敏感信息的安全。《密码法》已于 2020 年 1 月 1 日生效，其第二十二条强调了建立和完善商用密码标准体系的要求、第二十四条直接指出了“商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。”可以看出，密码管理相关国家标准的重要性。企业应予以学习、研究和应用。

主要变化四：将“隐私政策”调整为“个人信息保护政策”

【条文对比】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
5.5 隐私政策 ……	5.5 个人信息保护政策 …… 注 1：组织会习惯性将个人信息保护政策命名为“隐私政策”或其他名称，其内容宜与个人信息保护政策内容保持一致。

【解读】:《规范》（2020 正式版）将过去版本使用的“隐私政策”和实践中习惯使用的“隐私政策”调整为了“个人信息保护政策”。

从“隐私政策”调整为“个人信息保护政策”，原因有二：

一、个人信息与隐私的范围不一致，对此基本达成了共识。《民法典》（草案）第四编人格权第六章的名称为“隐私权和个人信息保护”，将隐私权和个人信息保护进行了明确区分，其中第一千零三十二条第二款规定“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”，第一千零三十四条第二款规定“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，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱地址、行踪信息等。”而对一千零三十四条第三款则更加直接地说明了隐私和个人信息的关系，“个人信息中的私密信息，同时适用隐私权保护的有关规定。”也就是说，个人信息中的私密信息属于隐私信息，除私密信息外的个人信息不属于隐私信息。

二、实践中惯用的“隐私政策”，规定的内容实际是对个人信息的保护政策，而非专门针对隐私的保护政策。翻阅各个网站、App 的隐私政策，其内容基本围绕对全部个人信息的收集、使用、存储、对外提供、个人信息主体权利保护等个人信息的相关保护内容，而对仅针对隐私信息。

因此，从“隐私政策”调整为“个人信息保护政策”，表面上是对政策文本名称的简单变化，但实际上确实将政策文本的适用范围界定得更加严谨、准确。

主要变化五：将个人信息主体的权利作为专门的条款要求

【条文对比】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
7 个人信息的使用 …… 7.8 个人信息查询 7.9 个人信息更正 7.10 个人信息删除 7.11 个人信息主体撤回授权同意 7.12 个人信息主体注销账户 7.13 个人信息主体获取个人信息副本 7.14 响应个人信息主体的请求 7.15 投诉管理	8 个人信息主体的权利 8.1 个人信息查询 8.2 个人信息更正 8.3 个人信息删除 8.4 个人信息主体撤回授权同意 8.5 个人信息主体注销账户 8.6 个人信息主体获取个人信息副本 8.7 响应个人信息主体的请求 8.8 投诉管理

【解读】:《规范》（2020 正式稿）将个人信息主体的权利相关内容，从原来的放置在“个人信息的使用”版块下调整为作为单独条款，结构更加严谨、个人信息主体权利相关内容更加突出。这样的行文安排，与《网络安全法》分别将个人信息使用相关要求规定在第四十一条、将个人信息主体权利相关要求规定在第四十三条，《App 违法违规收集使用个人信息行为认定方法》分别将个人信息使用相关要求规定在第三条、将个人信息主体权利相关要求规定在第六条的立法思路保持一致。

主要变化六：优化个人信息主体注销账户的相关规定

【条文对比】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
7.12 个人信息主体注销账户 对个人信息控制者的要求包括： …… c) 受理注销账号请求后，需要人工处理的，应在承诺时限内（原则上不超过十五天）完成核查和处理； …… e) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为必要注销条件等；	8.5 个人信息主体注销账户 对个人信息控制者的要求包括： …… b) 受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过 15 个工作日）完成核查和处理； …… d) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等； 注 1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明。 注 2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除并切断账户体系与产品或服务的关联等措施实现注销。

【解读】:《规范》（2020 正式稿）放宽了人工处理注销账号的时间要求，提高了“不应注销单个账户视同注销多个产品或服务”的可执行性。

从人工处理注销账号的时间要求看，《规范》（2020 正式稿）将时限从十五天放宽至十五个工作日，与《App 违法违规收集使用个人信息行为认定方法》第 6.3 条保持基本一致，有利于企业更好地处理用户注销过程中遇到的复杂问题。

对于提高“不应注销单个账户视同注销多个产品或服务”的可执行性，有助于更好地缓

解实践中集团使用一个通用账号下，在现有账号体系下如果注销一个账号确实可能导致的注销多个产品或服务的矛盾。实践中，有部分企业，为了方便用户登录、提高用户使用集团内部不同产品或服务的便利，费了周折后打通了账号体系，使用通用账号可以登录集团内部所有的产品或服务。该等通用账号其出发点是好的，但其确实与用户注销账号时注销一个通用账号可能导致该集团所有产品或服务都无法使用产生了矛盾，而用户注销账号的本意可能也只是不想使用某一个产品或服务。从用户体验角度，注销一个账号导致所有产品或服务都无法使用，用户可能会产生“被逼迫”或者“店大欺客”的想法。对此，《规范》（2020 正式稿）增加了两个注的内容，提供了可行性的执行建议。

主要变化七：放宽第三方接入管理的部分要求

【条文对比】

《规范（征求意见稿）》 （2019.10.22 版）	《规范》 （2020 正式稿）
8.7 第三方接入管理 …… e) 应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，核验其实现的方式； f) 应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，~~并妥善留存、及时更新，~~以供个人信息主体查询、使用； ……	9.7 第三方接入管理 …… e) 应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式； f) 应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用； ……

【解读】：《规范》（2020 正式稿）放宽了第三方接入管理中对于核验第三方征得个人信息主体同意的方式的要求，删去了“妥善留存、及时更新第三方产品或服务建立响应个人信息主体请求和投诉等的机制”的要求。

从放宽了第三方接入管理中对于核验第三方征得个人信息主体同意的方式的要求看，只有在必要时企业才需要进行核验，而不再要求必须核验，一定程度上减轻了企业的负担。对于“必要”的理解，宜理解为收到用户对于第三方未经同意收集使用个人信息的投诉、第三方被爆出违法违规收集使用的相关新闻或者监管通报第三方存在违法违规收集使用个人信息等情形。

从删去“妥善留存、及时更新第三方产品或服务建立响应个人信息主体请求和投诉等的机制”的要求看，减少了可能产生的歧义理解和操作中的困难，将确保个人信息主体能够表

达权利请求和投诉等的要求，强化在了第三方这一主体身上。

主要变化八：放宽任命专职个人信息保护负责人和个人信息保护工作机构的部分条件

【条文对比】

《规范（征求意见稿）》（2019.10.22 版）	《规范》（2020 正式稿）
10.1 明确责任部门或人员 …… c) 满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作： 1) 主要业务涉及个人信息处理，且从业人员规模大于 200 人； 2) 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息； 3) 处理个人敏感信息的。 ……	11.1 明确责任部门或人员 …… c) 满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作： 1) 主要业务涉及个人信息处理，且从业人员规模大于 200 人； 2) 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息； 3) 处理超过 10 万人的个人敏感信息的。 ……

【解读】：《规范》（2020 正式稿）将处理个人敏感信息即需要设立专职的个人信息保护负责人和个人信息保护工作机构，放宽至处理超过 10 万人的个人敏感信息。实践中，并非多数企业都能触发列举的前两个从业人员规模、处理个人信息数量要求，但一般来说，涉及收集使用个人信息的企业，大多数都会涉及到处理个人敏感信息。如果按照处理个人敏感信息即需要设立专职的要求，可以说，多数企业均需要设置个人信息保护专职负责人和工作机构。而放宽至处理超过 10 万人的个人敏感信息，能够将一部分企业筛除在外，提高了该等要求的可执行性和科学性。

主要变化九：新增建立自动化审计系统的要求

【条文对比】

《规范（征求意见稿）》（2019.10.22 版）	《规范》（2020 正式稿）
10.7 安全审计 …… b) 应~~采取~~建立自动化审计系统~~等方式~~，监测记录个人信息处理活动； ……	11.7 安全审计 …… b) 应建立自动化审计系统，监测记录个人信息处理活动； ……

【解读】：《规范》（2020 正式稿）在第 11.3 条沿用了此前对于个人信息处理活动记录的要求，在第 11.7 条新增建立自动化审计系统的要求，旨在为监测记录个人信息处理活动提

供技术保障。对于自动化审计系统的理解，以个人信息存储在云上为例，部分云服务商提供了数据库审计的服务，可以考虑作为这里的自动化审计系统使用。但是否确切符合《规范》（2020 正式稿）规定的自动化审计系统要求，有待监管部门的进一步意见。

第二部分、企业最关心的两大问题

问题一：《个人信息安全规范》GB/T 35273-2020 的修订历程

问题二：《个人信息安全规范》GB/T 35273-2020 的效力

与《个人信息安全规范》GB/T 35273-2017 一样，《规范》（2020 正式稿）仍然为推荐性国家标准，不具有强制执行力。但相信随着《个人信息安全规范》GB/T 35273-2017 的发布和实施，大家已经充分认识到《个人信息安全规范》的实际影响力。

正如《个人信息安全规范》第 1 条范围中指出的“本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估”，《个人信息安全规范》的作用和影响包括但不限于：

第一，《个人信息安全规范》是监管部门开展 App 相关执法工作的重要依据。2019 年 3 月 15 日，市场监管总局、中央网信办公告决定开展 App 安全认证工作。在监管部门公开的《移动互联网应用程序（App）安全认证实施规则》中，《个人信息安全规范》及相关标准、规范被确定为 App 安全认证的认证依据，明确将被用于 App 安全认证工作之中，充分体现了监管部门对《个人信息安全规范》等相关标准的认可态度。

第二，《个人信息安全规范》也是个人信息保护相关立法文件的重要参考。2019 年出台的《App 违法违规收集使用个人信息自评估指南》、《儿童个人信息网络保护规定》、《App 违法违规收集使用个人信息行为认定方法》等正式文件和《数据安全管理办法（征求意见稿）》等相关规定的征求意见稿，均在一定程度上沿用了《个人信息安全规范》对个人信息控制者的相关要求及背后的立法精神。

结语：《个人信息安全规范》（GB/T 35273-2020）的正式发布，一定程度上反映了个人信息保护相关问题的最新监管态度，同时对最新形势下个人信息保护面临的问题，直接进行了响应并提出了有益的合规参考。可以说，继《个人信息安全规范》（GB/T 35273-2017）之后，《个人信息安全规范》（GB/T 35273-2020）将开启我国个人信息保护工作的新篇章。建议各企业高度重视《个人信息安全规范》（GB/T 35273-2020）的相关规定，系统对照和梳理个人信息保护工作的开展现状，尽快开展查漏补缺，切实提高个人信息保护的能力，更好地满足个人信息保护的合规要求。（来源：威科先行法律信息库）

四、政府之声

➢ 工信部印发《工业数据分类分级指南（试行）》的通知

2020 年 3 月 4 日，工业和信息化部办公厅印发了《工业数据分类分级指南(试行)》(以下简称《指南》)。现将《指南》有关内容解读如下。

问：《指南》出台的背景是什么，对于支撑企业数字化转型发展具有哪些意义？

答：党中央、国务院高度重视大数据在推动数字经济发展中的作用。习近平总书记在十九大报告中强调要推动互联网、大数据、人工智能和实体经济深度融合,在十九届中央政治局第二次集体学习中提出要实施国家大数据战略，构建以数据为关键要素的数字经济。十九届四中全会首次提出将“数据”作为生产要素参与分配，这为数据赋予了新的历史使命。国务院印发《促进大数据发展行动纲要》，要求全面推进我国大数据发展和应用，加快建设数据强国，释放技术红利、制度红利和创新红利。

当前，我国大数据技术在工业领域用户需求精准分析、生产过程改进优化、营销管理智能决策等方面的应用方兴未艾。工业数据作为新的生产要素资源，支撑供给侧结构性改革、驱动制造业转型升级的作用日益显现，正成为推动质量变革、效率变革、动力变革的新引擎。但与此同时，工业数据也存在管理执行不到位、开发利用不深入、流通共享不充分等问题，尚未完全发挥对数字经济的放大、叠加和倍增作用。

工业数据分类分级是提升企业数据管理水平的基础，是有效挖掘数据价值、实现企业生

产方式变革的必由路径。《大数据产业发展规划(2016-2020 年)》将分类分级作为数据管理要点。《工业控制系统信息安全防护指南》提出对数据进行分级分类管理。《数据管理能力成熟度评估模型》(GB/T 36073-2018，以下简称 DCMM)明确将数据分类分级作为数据管理能力第 2 级(受管理级)至第 5 级(优化级)的基本要求。因此，亟需制定工业数据分类分级指导性文件。

问：《指南》的定位是如何考虑的，主要内容有哪些?

答：《指南》旨在指导企业全面梳理自身工业数据，提升数据分级管理能力，促进数据充分使用、全局流动和有序共享。一是明确企业为数据分类分级主体。工业企业、工业互联网平台企业等作为工业数据的所有者和使用者，承担开展数据分类分级、加强数据管理等主体责任。二是与 DCMM 互为补充、相互衔接。《指南》将与 DCMM 贯标工作有机结合，引导企业通过数据防护技术应用、管理流程优化、组织体系变革等方式，实现工业数据管理能力跃升。三是以可操作、可实施为原则持续完善。为确保《指南》内容的有效性和适应性，拟以实践效果为导向，在试点工作中不断改进优化，适时予以修订。

《指南》共 4 章 16 条，主要内容包括：第一章总则，阐述编制目的及依据，提出工业数据的基本概念，明确适用范围和原则;第二章数据分类，企业结合行业要求、业务规模、数据复杂程度等实际情况，围绕数据域进行类别梳理，形成分类清单;第三章数据分级，按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为 3 个级别;第四章分级管理，针对有关主管部门和企业建立数据管理制度、实施差异化管理进行描述，为 DCMM 贯标等提供参考依据。

问：各方应该如何落实《指南》，共同促进工业数据管理水平的提升?

答：企业应落实工业数据分类分级主体责任。一是制度要“实”，企业要建立健全工业数据分类分级管理制度，明确信息化部门、生产部门、行政部门等多方协同的工作机制。二是梳理要“全”，按照纵向贯穿管理层至控制层、横向覆盖全流程环节的原则，围绕数据域全面实施数据分类，形成企业工业数据清单。三是分析要“准”，鉴于不同行业、不同规模的企业因数据受损所致后果的评价标准、承受能力均存在差异，建议各行业、企业应结合自身实际，从有利于数据管理的角度，研究制定科学合理的量化定级指标。四是管理要“细”，切实做好对工业数据的差异化防护，不断完善数据管理措施，充分挖掘数据作为生产要素的潜在价值。

地方工业和信息化主管部门负责推动本辖区内工业数据分类分级工作，配合工业和信息化部做好宣贯培训、试点示范等相关工作。有关行业、领域管理部门可参考《指南》制定适

用本行业、本领域的标准或规范，为企业提供针对性指导。工业数据分类分级是一项较为复杂的系统性工作，《指南》是开展工业数据分级管理的基础规范，我们将根据试行期间各方反馈，不断完善相关内容，引导企业持续提升工业数据管理水平。（来源：工信部信息技术发展司）

- **《工业数据分类分级指南（试行）》工信厅信发〔2020〕6 号**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c7772152/content.html

➢ 教育部印发《2020 年教育信息化和网络安全工作要点》的通知

2020 年 3 月 3 日，日前，教育部办公厅印发《2020 年教育信息化和网络安全工作要点》（简称“《工作要点》”）的通知，对 2020 年教育信息化和网络安全重点工作进行了安排部署，主要包括工作思路、核心目标、重点任务三方面内容。

《工作要点》涵盖三个核心目标，一是全面落实党中央、国务院对教育领域网络安全和信息化的战略部署；二是深入实施教育信息化 2.0 行动计划；三是教育网络安全支撑体系不断完善，网络安全人才培养能力和质量全面提升，教育系统网络安全防护水平不断提高。

《工作要点》包括 11 大方面、32 项重点任务。包括：坚持党对教育信息化和网络安全工作的全面领导；有序开展数字资源服务普及行动；持续深化网络学习空间覆盖行动；协同实施网络扶智工程攻坚行动；全面推进教育治理能力优化行动；扎实开展百区千校万课引领行动；加快实施数字校园规范建设行动；稳步推进智慧教育创新发展行动；大力实施信息素养全面提升行动，强化教育信息化支撑保障措施；提升网络安全人才支撑和保障能力。

《工作要点》提出，加强教育信息化和网络安全工作统筹部署。研制教育信息化中长期发展规划、教育信息化“十四五”规划，出台推进“互联网+教育”发展的指导意见；落实新冠肺炎疫情防控总体部署，指导做好教育信息化和网络安全工作；完善中国教育和科研计算机网（CERNET）管理机制体制，健全 CERNET 主干网安全运行管理体系，保障 CERNET 安全稳定运行。

《工作要点》提出，遴选认定典型区域、标杆学校和典型课例。启动百区千校万课引领行动，遴选 30 个典型区域，300 所基础教育标杆学校、50 所职业教育标杆学校、30 所高等教育标杆学校、20 所继续教育标杆学校，3000 堂基础教育示范课例、200 堂职业教育示范课例、800 门国家精品在线开放课程、40 堂继续教育示范课例。

《工作要点》提出，推进 IPv6 规模部署行动。深入推进“互联网+”重大工程保障支撑类项目“面向教育领域的 IPv6 示范网络”项目（CERNET2 二期），支持 CERNET 主干网用户接入 IPv6。

《工作要点》提出，推动开展智慧教育创新示范。指导推进“智慧教育示范区”创建工作，开展 2019 年度创建区域绩效评估，遴选新增 5 个以上创建区域，探索开展智慧教育创新实践。（来源：中国教育网络）

➢ GB/T35273-2020《信息安全技术个人信息安全规范》正式发布

2020 年 3 月 6 日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 1 号）点击阅读原文查看全国信息安全标准化技术委员会归口的 GB/T35273-2020《信息安全技术个人信息安全规范》正式发布，并将于 2020 年 10 月 1 日实施。

序号	版本	时间
1	《个人信息安全规范》GB/T 35273-2017	2018.05.01 生效
2	《个人信息安全规范》（草案）	2019.02.01 征求意见
3	《个人信息安全规范》（征求意见稿）	2019.06.25 征求意见
4	《个人信息安全规范》（征求意见稿）	2019.10.24 公开（2019.10.22 版本）
5	《个人信息安全规范》GB/T 35273-2020	2020.10.01 生效

该标准代替 GB/T 35273-2017《信息安全技术 个人信息安全规范》，与 GB/T35273-2017 相比，主要技术变化如下：

一是，增加了“多项业务功能的自主选择”、“用户画像的使用限制”、“个性化展示的使用”、“基于不同业务目所收集个人信息的汇聚融合”、“第三方接入管理”、“个人信息安全工程”、“个人信息处理活动记录”等内容；

二是修改了“征得授权同意的例外”、“个人信息主体注销账户”、“明确责任部门与人员”、附录 C“实现个人信息主体自主意愿的方法”等内容。（来源：全国信息安全标准化技术委员会）

- **GB/T35273-2020《信息安全技术个人信息安全规范》**
- http://pip.tc260.org.cn/assets/wz/2020-03-07/ef2dab88-cd9d-4748-814a-a3eca027beba.pdf

➢ 工信部关于发布《网络安全标准实践指南—远程办公安全防护》的通知

2020 年 3 月 13 日，全国信息安全标准化技术委员会秘书处针对远程办公安全问题，组织相关厂商和安全专家，编制了《网络安全标准实践指南—远程办公安全防护》（以下简称《实践指南》）。

《实践指南》给出了远程办公的典型应用场景，分析了远程办公可能面临的办公系统自身安全、数据安全、设备安全和个人信息保护等风险，针对远程办公系统的使用方和用户，分别给出了安全控制措施建议。


全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE
搜索
首页 工作动态 行业观点 标准征求意见 标准查询 出版物 关于我们 平台登录
通知公告
关于发布《网络安全标准实践指南—远程办公安全防护》的通知
2020-03-13
信安秘字[2020] 12号
各有关单位：
全国信息安全标准化技术委员会秘书处针对远程办公安全问题，组织相关厂商和安全专家，编制了《网络安全标准实践指南—远程办公安全防护》（以下简称《实践指南》）。
《实践指南》给出了远程办公的典型应用场景，分析了远程办公可能面临的办公系统自身安全、数据安全、设备安全和个人信息保护等风险，针对远程办公系统的使用方和用户，分别给出了安全控制措施建议。其中，使用方应在管理和技术两方面开展安全防护，健全远程办公管理制度，加强运维管理，强化安全措施。用户应提高自身安全意识，重点针对设备、数据、环境等方面的安全风险进行防护。《实践指南》全文请点击附件下载。
附件：《网络安全标准实践指南—远程办公安全防护》.pdf

其中，使用方应在管理和技术两方面开展安全防护，健全远程办公管理制度，加强运维管理，强化安全措施。用户应提高自身安全意识，重点针对设备、数据、环境等方面的安全风险进行防护。（来源：全国信息安全标准化技术委员会秘书处）

- **《网络安全标准实践指南—远程办公安全防护》**
- https://www.tc260.org.cn/upload/2020-03-13/1584090952093076364.pdf

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 3 月安全更新

发布日期：2020-03-10
更新日期：2020-03-10
描述：CNTA-2020-0005

3 月 10 日，微软发布了 2020 年 3 月份的月度例行安全公告，修复了其多款产品存在的 407 个安全漏洞。受影响的产品包括：Windows 10 1909 & WindowsServer v1909（76 个）、Windows 10 1903 & WindowsServer v1903（75 个）、Windows 10 1809 & WindowsServer 2019（73 个）、Windows 8.1 & Server 2012 R2（55 个）、Windows RT 8.1（55 个）、Windows Server 2012（43 个）、Microsoft Edge (HTML based) (14 个)、Internet Explorer (6 个) 和 Microsoft Office-related software (10 个)。利用上述漏洞，攻击者可以提升权限，欺骗，绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-0684	**LNK 远程代码执行漏洞** Microsoft Windows 中存在远程代码执行漏洞，如果处理.LNK 文件，则该漏洞可能允许远程代码执行。成功利用此漏洞的攻击者可以获得与本地用户相同的用户权限。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 攻击者可以向用户提供包含恶意.LNK 文件和相关恶意二进制文件的可移动驱动器或远程共享。当用户在 Windows 资源管理器或任何其他解析.LNK 文件的应用程序中打开此驱动器（或远程共享）时，恶意二进制文件将在目标系统上执行攻击者选择的代码。安全更新通过更正快捷方式 LNK 引用的处理来解决该漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0801	**Media Foundation 内存破坏漏洞** 当 Windows Media Foundation 未能正确处理内存中的对象时，存在内存破坏漏洞。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 攻击者可以通过多种方式利用此漏洞，例如说服用户打开精心编制的文档，或说服用户访问恶意网页。 安全更新通过更正 Windows Media Foundation 如何处理内存中的对象来解决此漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909
CVE-2020	**GDI+远程代码执行漏洞** Windows Graphics Device Interface (GDI) 处理内存中对象的方式存在远程代码执行漏洞。成功利用此漏洞的	严重 远程执行代码	Windows 10 Server 2016 Server 2019

-0881	攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 安全更新通过更正 Windows GDI 处理内存中对象的方式来解决该漏洞。		Server, version 1803 Server, version 1909 Server, version 1903 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0787	**Windows Background Intelligent Transfer Service 权限提升漏洞** 当 Windows Background Intelligent Transfer Service (BITS)未能正确地处理符号链接时，存在权限提升漏洞。成功利用此漏洞的攻击者可以覆盖导致提升状态的目标文件。要利用此漏洞，攻击者首先必须登录到系统。然后，攻击者可以运行巧尽心思构建的应用程序，利用此漏洞并控制受影响的系统。 安全更新通过更正 Windows BITS 如何处理符号链接来解决该漏洞。	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0768	**Scripting Engine 内存破坏漏洞** 在 Microsoft 浏览器脚本引擎处理内存中对象的方式，存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 安全更新通过修改脚本引擎处理内存中对象的方式来解决该漏洞。	严重 远程执行代码	Edge (HTML based) Internet Explorer 11 ChakraCore
CVE-2020-0852	**Microsoft Word 远程代码执行漏洞** Microsoft Word 软件未能正确处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以使用精心编制的文件在当前用户的安全上下文中执行操作。例如，该文件可以代表与当前用户具有相同权限的登录用户执行操作。 安全更新通过更正 Microsoft Word 如何处理内存中的文件来解决此漏洞。	严重 远程执行代码	SharePoint Server 2019 Office 2019 Office Online Server Office 2016 for Mac
CVE-2020-0850	**Microsoft Word 远程代码执行漏洞** Microsoft Word 软件未能正确处理内存中的对象时存在远程代码执行漏洞。成功利用此漏洞的攻击者可以使用精心编制的文件在当前用户的安全上下文中执行操作。例如，该文件可以代表与当前用户具有相同权限的登录用户执行操作。 安全更新通过更正 Microsoft Word 如何处理内存中的文件来解决此漏洞。	重要 远程执行代码	SharePoint Enterprise Server 2016 SharePoint Enterprise Server 2013 SharePoint Server 2019 Office 2019 Office 2019 for Mac Office 365 ProPlus

			Office Online Server Word 2016 Office 2016 for Mac Word 2013 SharePoint Foundation 2013
CVE-2020-0891	**Microsoft SharePoint 反射型 XSS 漏洞** 此漏洞是由于 SharePoint 服务器未能正确过滤对受影响的 SharePoint 服务器的构建的请求而导致的。 经过身份验证的攻击者可以通过向受影响的 SharePoint 服务器发送构建的请求来利用此漏洞。成功利用此漏洞的攻击者可以对受影响的系统执行跨站点脚本攻击，并在当前用户的安全上下文中运行脚本。这些攻击可使攻击者读取未经授权读取的内容，使用受害者的身份代表受害者在 SharePoint 网站上执行操作，例如更改权限、删除内容、窃取敏感信息（如浏览器 cookies）以及在受害者的浏览器中注入恶意内容。 要利用此漏洞，用户必须单击构建的 URL，该 URL 将用户带到目标 SharePoint Web App 网站。	重要 欺骗	SharePoint Enterprise Server 2016 SharePoint Server 2019 SharePoint Foundation 2010 SharePoint Foundation 2013

➢ Cisco MDS 9000 Series Multilayer Switches NX-OS Software 拒绝服务漏洞

发布日期：2020-03-2
更新日期：2020-03-2
受影响系统：
Cisco MDS 9000 Series Multilayer Switches
描述：

CVE(CAN) ID: CVE-2020-3175
Cisco MDS 9000 Series Multilayer Switches 是美国思科（Cisco）公司的一款 MDS 9000 系列多层交换机。Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。
Cisco MDS 9000 Series Multilayer Switches 中的 NX-OS Software 的资源处理系统存在安全漏洞，该漏洞源于程序未能正确控制资源的使用。远程攻击者可通过快速向管理接口发送流量利用该漏洞造成拒绝服务（大量占用 CPU、进程崩溃或重启系统）。
<*来源：Cisco
建议：

厂商补丁：
Cisco
目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-nxos-cdp

➢ WPS Office 存在 dll 劫持漏洞

发布日期：2020-3-5
更新日期：2020-3-5
受影响系统：
WPS Office 11.1.0.9339
描述：

CVE(CAN) ID: CNVD-2020-10216
WPS Office 是金山办公软件出品的 office 软件,可以实现办公软件常用的文字、表格、演示等多种功能。
WPS Office 存在 dll 劫持漏洞，攻击者可以利用漏洞加载恶意 dll，执行恶意代码。
<*来源：珠海金山办公软件有限公司
建议：

厂商补丁：
珠海金山办公软件有限公司
厂商暂未提供漏洞修复方案，请关注厂商主页更新：
https://www.wps.cn/

➢ Cloud Foundry Cloud Controller 未授权访问漏洞

发布日期：2020-03-2
更新日期：2020-03-2
受影响系统：
Cloud Foundry Cloud Controller <1.91.0
描述：

CVE(CAN) ID: CVE-2020-5400
Cloud Foundry 是美国 Cloud Foundry 基金会的一套开源的平台即服务（PaaS）云计算平台。该产品提供容器调度、持续交付和自动化服务部署等功能。Cloud Controller 是其中的一款云控制器。
Cloud Foundry Cloud Controller (CAPI) 1.91.0 之前版本中存在安全漏洞。攻击者可利用该漏洞获取凭证，进而未授权访问被保护的资源。
<*来源：Cloud Foundry
建议：

厂商补丁：
Cloud Foundry

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.cloudfoundry.org/blog/cve-2020-5400

六、本期网络安全事件

➢ 英国电信企业 Virgin Media 数据泄漏 暴露了 90 万名客户详细信息

2020 年 3 月 6 日，近日，维珍传媒披露了一次数据泄露事件，表示泄露了大约 90 万名客户的个人信息（涉及姓名、家庭、电子邮件地址和电话号码等）。未知身份的外来访问者对一个配置错误的不安全的营销数据库进行了非法访问。

维珍传媒是英国和爱尔兰知名的有线电视运营商，截至 2019 年 12 月 31 日，该公司为约 600 万有线电视用户提供电话、电视和互联网服务，并为 330 万订阅用户提供移动服务。

该公司于 2020 年 2 月 28 日发现了这一安全漏洞，并确定数据库从 2019 年 4 月 19 日就可以被访问。根据一项正在进行的安全调查，该数据库最近才被未经授权的第三方至少访问过一次。维珍传媒立即下线了对这个暴露在公网的数据库，解决了这个安全问题。

维珍传媒首席执行官 Lutz Schüle 在新闻发布会上说：“我们最近发现，一个营销数据库出现配置错误，可让第三方在未经授权的情况下访问。我们立即解决了这个问题，下线了这个数据库，其中包含了大约 90 万人的一些联系信息，涉及固定电话客户，大约占该客户群的 15%。保护我们客户的数据是我们的首要任务，为此我们真诚地道歉。”

该公司 CEO 还指出，该数据库不包括财务信息或帐户密码。

维珍媒体正在联系受影响的客户，建议他们对可能发生的钓鱼攻击保持警惕。“我们正在联系那些受影响的客户，告诉他们发生了什么。我们建议所有人在点击未知链接或向未知第三方提供信息之前保持谨慎。”

在一个单独的数据泄露通知页面上，该公司提供了关于该事件的更多细节，它显示了该数据库所包含的维珍传媒客户信息的条目，例如：联系方式（姓名、家庭和电子邮件地址以及电话号码）、技术及产品资料、客户的出生日期（极少数情况）。

近期，美国无线运营商 T-Mobile 也披露了一个数据泄露事件，同样涉及了一些客户的个人信息。（来源：Pierluigi Paganini）

➢ 团伙冒充农商行行长行骗被当场识破！竟有银行“内鬼”从旁协助

2020 年 3 月 11 日北青金融报道，2019 年 4 月 20 日，一对男女在商水农商行营业大厅冒充该行行长和工作人员行骗，被商水农商行工作人员当场识破。

值得注意的是，在此次颇为拙劣的团伙行骗过程中，竟有银行“内鬼”从旁策应。根据裁判文书网 3 月 9 日披露的刑事判决书，3 名涉案的犯罪嫌疑人中，苗广福、郭改正均为河南省周口市商水县农民，而郭长征为商水农商行汤庄支行内退员工。

苗广福、郭改正诈骗二审刑事判决书

发布日期：2020-03-09　　浏览：50次

河南省周口市中级人民法院

刑 事 判 决 书

（2020）豫16刑终108号

原公诉机关商水县人民检察院。

上诉人（原审被告人）苗广福，男，汉族，1957年12月9日出生，初中文化，农民，户籍所在地河南省驻马店市西平县，捕前住河南省西平县。因犯诈骗罪，于2007年12月21日被河南省漯河市源汇区人民法院判处有期徒刑一年零六个月，并处罚金人民币一万元。因涉嫌诈骗犯罪，于2019年4月20日被商水县公安局刑事拘留，同年5月25日被逮捕。

经法院审理查明，2018 年 12 月份，郭改正经人介绍与被害人罗某相识，郭改正自称是商水农商行主任，能办理企业借款保函。后郭改正、郭长征预谋给罗某办假“借款保函”。

2019 年 4 月 19 日上午，“张玉梅”（女）和郭改正、苗广福、郭长征四人在商水农商行南见面，郭改正将事先准备的假身份证、文件和印章交给苗广福，后张玉梅和苗广福、郭长征协商，让郭改正向罗某索要现金人民币 4 万元，当日下午 14 时许，被告人郭改正以办理保函需要费用为由，在商水县“金汇国际酒店”511 房间内，骗取被害人罗某现金人民币 4 万元。后由苗广福和“张玉梅”分别冒充商水农商行行长李楠和银行工作人员，在商水农商行营业大厅与被害人罗某等人见面，在办理假借款保函过程中，被告人苗广福身份被识破，银行工作人员报警后，苗广福被抓，“张玉梅”趁机逃走。

据悉，侦察机关从苗广福携带的档案袋里发现伪造的李楠的身份证一个、商水农商行的公章一枚、商水农商行的部分红头文件。郭改正于案发当晚和次日凌晨通过 ATM 机退款给罗某 39000 元。经鉴定，印章与商水农商行印章不是同一枚印章。

根据上述事实和证据，法院作出如下判决：被告人苗广福犯诈骗罪，判处有期徒刑二年，并处罚金人民币一万五千元；被告人郭改正犯诈骗罪，判处有期徒刑二年，缓刑三年，并处罚金人民币一万五千元；被告人郭长征犯诈骗罪，判处有期徒刑二年，缓刑三年，并处罚金人民币一万五千元。（来源：北青金融）

➢ 英国多个火车站免费 Wi-Fi 暴露用户数据

2020 年 3 月 3 日，Security Discovery 的一名研究人员发现，与英国多个火车站的免费 Wi-Fi 热点连接的用户数据已存储在非密码保护的数据库中。该数据库包含 1.46 亿条记录，其中包括电子邮件地址，年龄范围，旅行原因，设备数据和其他日志。

运营数据库的 C3UK 在 2 月 14 日星期五（即报告的同一天）限制了对数据库的公共访

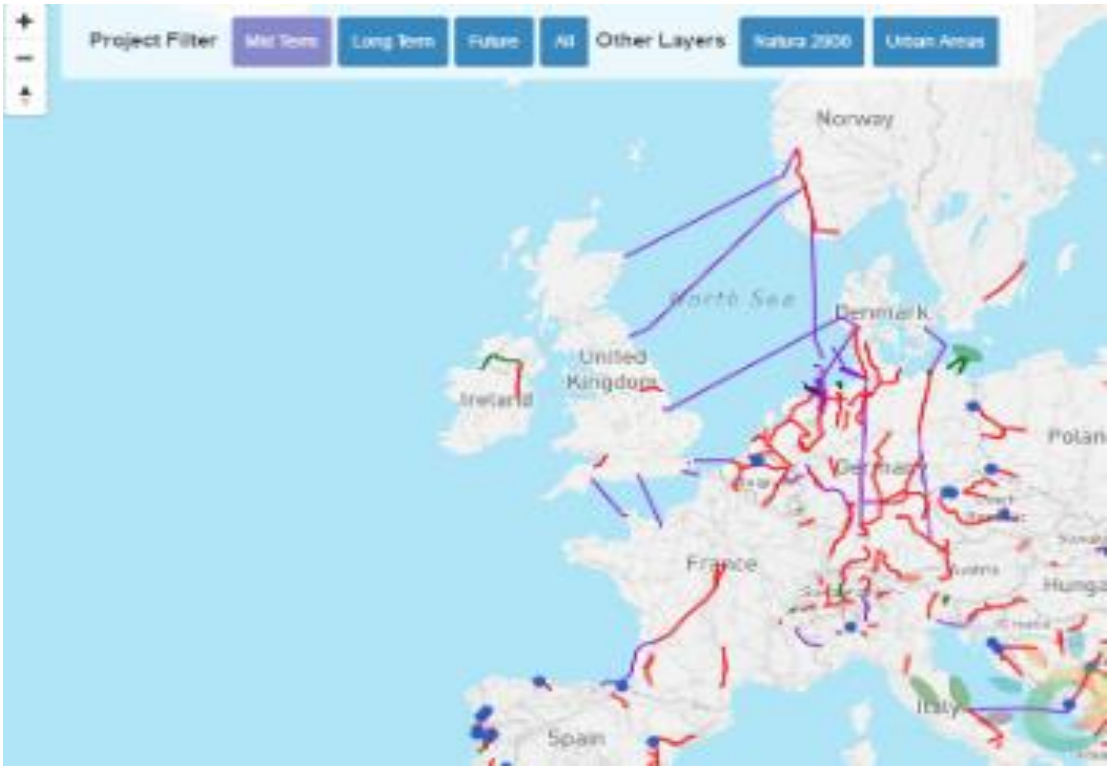
问。据发现这一问题的耶利米·福勒（Jeremiah Fowler）说，这样公开的电子邮件数据库增加了针对性网络钓鱼攻击的风险。

研究人员表示，许多人使用他们的真实姓名作为电子邮件地址的一部分，并进一步暴露他们的个人身份。在这种情况下，任何有互联网连接的人都可以看到用户所在的站点、时间戳、他们可能看到的广告、他们居住的邮政编码等等。每一条信息基本上都是一个拼图块，可以用来描绘用户的真实身份。

随着越来越多的免费 Wi-Fi 热点开始出现在城镇周围，提供商和消费者都将不得不开始思考如何更好地保护数据。对于最终用户来说，使用 Jigsaw 的 Intra 或虚拟专用网络等工具可以更好地保护数据。（来源：cnBeta）

➢ 欧洲高压电网监督组织 ENTSO-E 被黑客成功入侵

2020 年 3 月 12 日，负责监督欧洲高压电力基础设施运行的组织 ENTSO-E 被黑客成功入侵了。ENTSO-E 成立于 2008 年，由 35 个成员国的 42 个传输系统运营商(TSO)组成。TSO 运行高压电力网络，为包括发电机和配电商在内的客户提供电网接入。它们对于保持整个欧洲的电力运转至关重要，而监管的关注也越来越集中在其网络安全上。



该组织在 3 月 9 日简短地说：“最近发现了成功侵入其办公网络的证据”。ENTSO-E 的任

务包括“协调关键基础设施的保护措施”和“开发和维护通信基础设施”，其中包括实时数据交换通信网络。ENTSO-E 秘书长 Laurent Schmitt 在 1 月份指出，“解决电网网络安全问题确实是复杂的火箭科学，需要开展跨职能协作。”

欧盟电网组织被黑客入侵的结果就是“无法连接运营的 TSO 系统”。

ENTSO-E 本周表示：“重要的是，请注意 ENTSO-E 办公网络未连接到任何可运行的 TSO 系统。我们的 TSO 成员已获悉，我们将继续监视和评估情况。目前，已经进行了风险评估，并制定了应急计划以减少任何进一步袭击的风险和影响。”该组织没有共享有关入侵类型的详细信息。

芬兰 TSO Fingrid 说：“由于这次安全攻击，Fingrid 发出的 EIC 代码的时间可能比平时更长。”(EIC 代码是欧洲使用的 16 个字符的代码，用于标识参与跨界电力和天然气交易的实体)。

Fingrid 补充说：“该事件仅影响 Fingrid 和 ENTSO-E 之间的文件交换策略。”ENTSO-E 无疑将成为寻求市场情报以及潜在敌意侦察的组织的诱人目标。

安全公司 Dragos 指出，攻击者以前的目标是供应商，承包商和其他实体之间的可信连接以及最终目标。“ENTSO-E 不管理或控制任何工业资产，但出于监管或类似原因而链接到各种 ICS 实体。基于这种联系，可以利用对一个受害实体的成功入侵来促进受支持的公用事业组织的后续访问或利用。”

欧盟网络安全网络(ENCS)强调说：“TSO 运行着一些最关键的关键基础设施，跨越距离和边界传输电力并保持电网平衡。如果他们受到网络攻击的危害，那么引起的停电规模是相当大的。（来源：电缆网）

➢ 真假班主任！警方发现嫌疑犯 3 人联合上演“大戏”骗钱财

2020 年 3 月 10 日，受疫情影响，今年各地学校延迟开学，家长 QQ 群、微信群成了老师与学生家长沟通的平台。然而一些不法分子也瞄上了家长群，他们费尽心思混进群里，时而冒充某某学生的家长、时而冒充班主任，不同角色之间切换自如，他们来的目的只有一个就是收钱。

2 月 15 日，在湖北省襄阳市樊城区某中学初三的班级微信群里，一个标注为班主任黄老师的微信号发布了一则收费通知，要求家长尽快缴纳新学期的资料费 750 元。一看是班主

任发布的通知，很多家长第一时间向对方提供的收款码转账。就在此时，另一个与班主任黄老师头像和名字相同的微信号也发了一条信息，要求家长立即停止转账。一会要求转账，一会却又禁止转账，相同的头像、相同的名字，到底谁是真正的班主任黄老师呢?

此时，襄阳市公安局 110 指挥中心接到了这所学校的报案。通过警方核实，后来在群里要求家长停止转账的那个黄老师才是真正的班主任。

民警通过犯罪嫌疑人留下的二维码信息着手进行调查，梳理查证了 20 多个银行账户及三方支付的资金流、信息流，最终锁定了 3 名来自广西的犯罪嫌疑人。2 月 20 日，在广西公安机关的积极协作下，犯罪嫌疑人宁某、张某、彭某到案，现场查获多部作案使用的手机、现金等物品。除了冒充班主任，为了能让家长们相信，另外两名犯罪嫌疑人冒充学生家长。不管这个假班主任发布什么信息，这两名假家长都会积极迎合，从而达到诈骗的目的。

此类案件并非个例

2 月 29 日，发生在江苏省南京市六合区的案件，一家幼儿园的家长群被犯罪嫌疑人盯上了。据幼儿园老师曹女士回忆，2 月中旬，一名男子自称是她班级里一位学生的家长，申请加入了她们幼儿园的家长 QQ 群，在报出了孩子的个人信息资料后，这名男子顺利取得了老师的信任并入了群。

在潜伏几天之后，这名男子将自己的 QQ 头像和昵称改成了幼儿园生活老师的头像，并模仿老师的口气在群里发布了收取 3800 元学费的信息，并同时在群里发布了一个收款二维码。而这个信息在群内发布仅仅两分钟的时间，就有多名家长进行了确认回复。

幼儿园老师将骗子踢出 QQ 群并报了警，同时，尽快电话联系每一位家长，告知他们不

要上当。而由于幼儿园的迅速处置，骗子这次没有骗到一分钱。

针对此类诈骗案件多发的情况

2020 年 2 月 17 日，教育部全国治理教育乱收费联席会议办公室发布关于谨防有人利用疫情防控期间线上教学名义进行网上收费诈骗的预警。建议广大中小学生和家长，在积极做好疫情防控、有序开展线上学习的同时，对借此名义收取相关费用的行为，一定要提高警惕，增强防范意识，以免上当受骗，遭受不必要的经济损失。一旦发现可疑情况，应及时向学校和老师反映，并保存好相关证据、及时报警。

各级教育部门和学校要按照“谁主管谁负责、谁开发谁负责、谁选用谁负责”的原则，认真落实教育移动互联网应用程序的网络安全主体责任，建立健全教育移动应用管理责任体系，切实维护广大师生和家长的切身利益。对学校和班级建立的微信群、QQ 群等，要严格落实群主管理责任，严格核实所有成员身份，严格落实实名制度，严格入群批准验证，杜绝陌生人随意入群现象，对身份存疑的尽快清除出群。对确有需要通过网上支付的合规收费事项，建议学生和家长要与学校和老师进行确认，不可盲目进行网上支付。

对此，警方也提示，凡是入群人员，都要做到四点：

一看：看申请人员真实身份。

二开：开启入群验证信息。

三查：查可疑账号发布内容。

四核：核实缴费信息。 （来源：央视新闻）

➢ 厦门银行 APP 遭"00 后"黑客非法入侵 建行手机 APP 也中招

2020 年 3 月 6 日，2000 年出生的田某，尽管只有初中文化，却有着极强的计算机天赋，并将手伸向了系统防卫森严的银行机构。

具体来看作案过程

2019 年 1 月 5 日初，田某通过软件抓包、PS 身份证等非法手段，在厦门银行手机银行 APP 内使用虚假身份信息注册银行Ⅱ、Ⅲ类账户。其在注册账户过程中，田某先输入本人身份信息，待进行人脸识别步骤时，利用软件抓包技术将银行系统下发的人脸识别身份认证数据包进行拦截并保存。尔后，在输入开卡密码步骤，被告人田某将 APP 返回到第一步(上传身份证照片之步骤)，输入伪造的身份信息，并再次进入到人脸识别之身份验证步

骤。此时，其上传此前拦截下来的包含其本人的身份信息数据包，使系统误以为要比对其本人的身份信息，其遂用本人人脸通过银行系统人脸识别比对，使得成功利用虚假身份信息注册到银行账户。

利用上述方法，田某成功注册厦门银行 II 类账户 76 个。其将上述账户信息(包括身份证号、银行卡号、绑定的手机号)卖给被告人多人，可证实获利金额为人民币 22010 元。因手机银行存在漏洞被田某利用，致使厦门银行从 2019 年 1 月 18 日开始，一直关闭手机银行 APP 软件中 II 、III类账户开户链接功能。

在贩卖账号过程中，田某结实了张某

张某，1995 年出生，小学文化。起初，张某只是从田某手中购买账户。为赚取更多利润，张某向他人学习上述软件抓包技术，并使用该技术在多家银行尝试注册 II 、III类账户。其中，被告人张某利用该技术在厦门银行 APP 上拦截身份认证信息数次，在建设银行 APP 上使用拦截身份认证信息十余次，在浦发银行极速开户网页页面拦截身份认证信息

四、五次。此外，被告人张某花费人民币 1888 元雇请他人利用上述软件抓包技术，在建设银行系统内成功注册 12 个Ⅱ、Ⅲ类账户。

2019 年 3 月 18 日，田某在河南商丘被公安人员抓获;次月，张某在黑龙江哈尔滨被公安人员抓获。该案最终在厦门市思明区人民法院开庭审理，法院认为，被告人田某、张某犯非法获取计算机信息系统数据罪的事实清楚，证据确实、充分。法院一审判决：被告人田某犯非法获取计算机信息系统数据罪，判处有期徒刑三年，并处罚金人民币一万元;被告人张某犯非法获取计算机信息系统数据罪，判处有期徒七个月，并处罚金人民币五千元。

（来源：和讯网）