国盟信息安全通报

2019 年 7 月 22 日第 197 期

国盟信息安全通报

（第 197 期）

国际信息安全学习联盟

2019 年 7 月 22 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 316 个，其中高危漏洞 123 个、中危漏洞 170 个、低危漏洞 23 个。漏洞平均分值为 6.42。本周收录的漏洞中，涉及 0day 漏洞 157 个（占 50%），其中互联网上出现“WordPress CRUDLab WP LikeButton 插件身份验证漏洞、D-Link DIR-818LW 命令注入漏洞（CNVD-2019-22213）”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 2528 个，与上周（3353 个）环比下降 25%。

主要内容

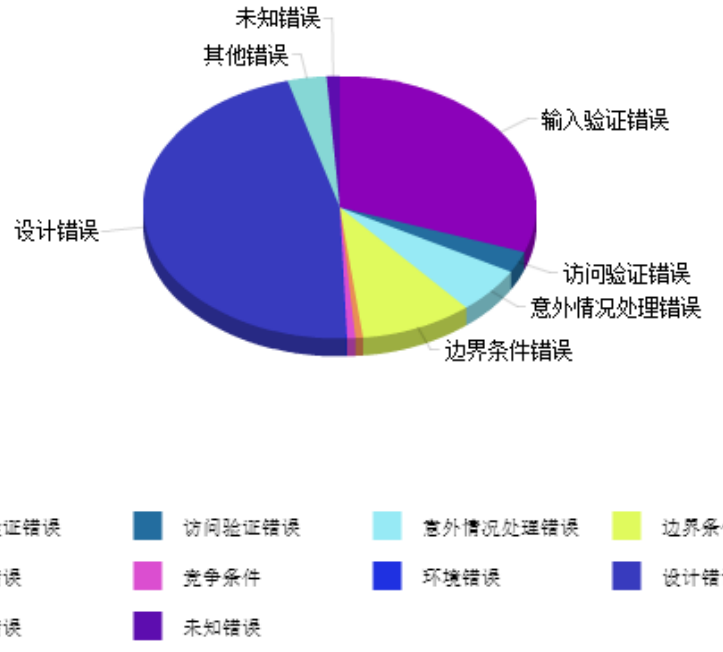
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

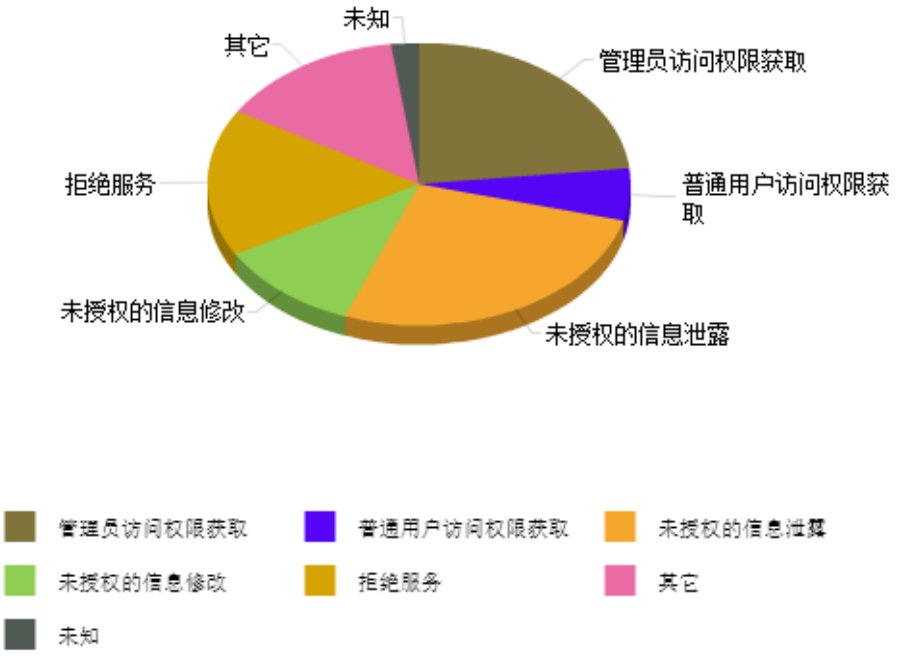
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 316 个，其中高危漏洞 123 个、中危漏洞 170 个、低危漏洞 23 个。漏洞平均分值为 6.42。本周收录的漏洞中，涉及 0day 漏洞 157 个（占 50%），其中互联网上出现“WordPress CRUDLab WP LikeButton 插件身份验证漏洞、D-Link DIR-818LW 命令注入漏洞（CNVD-2019-22213）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2528 个，与上周（3353 个）环比下降 25%。

二、安全漏洞增长数量及种类分布情况

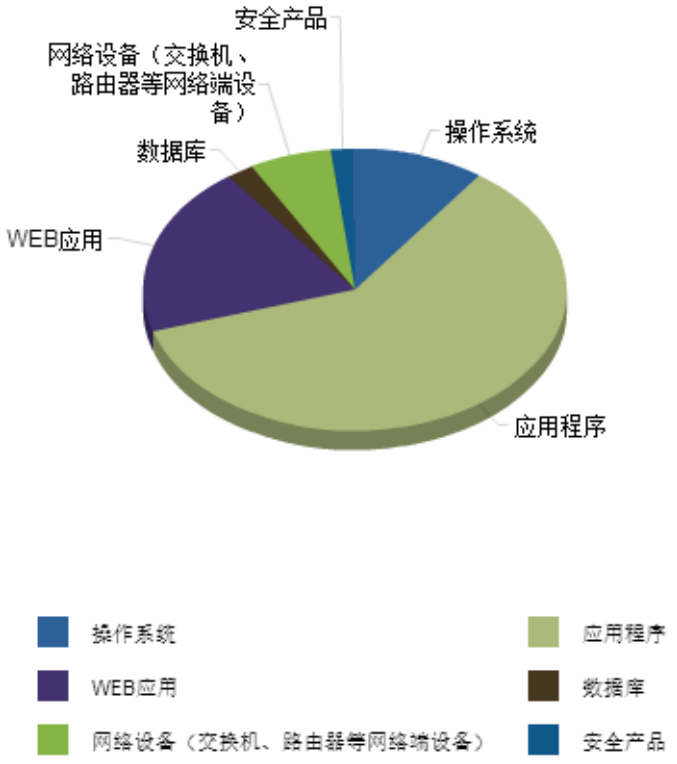
➢ 漏洞产生原因（2019 年 7 月 8 日—2019 年 7 月 22）



➢ 漏洞引发的威胁（2019 年 7 月 8 日—2019 年 7 月 22）



➢ 漏洞影响对象类型（2019 年 7 月 8 日—2019 年 7 月 22）



三、安全产业动态

➢ 网络诚信建设刻不容缓

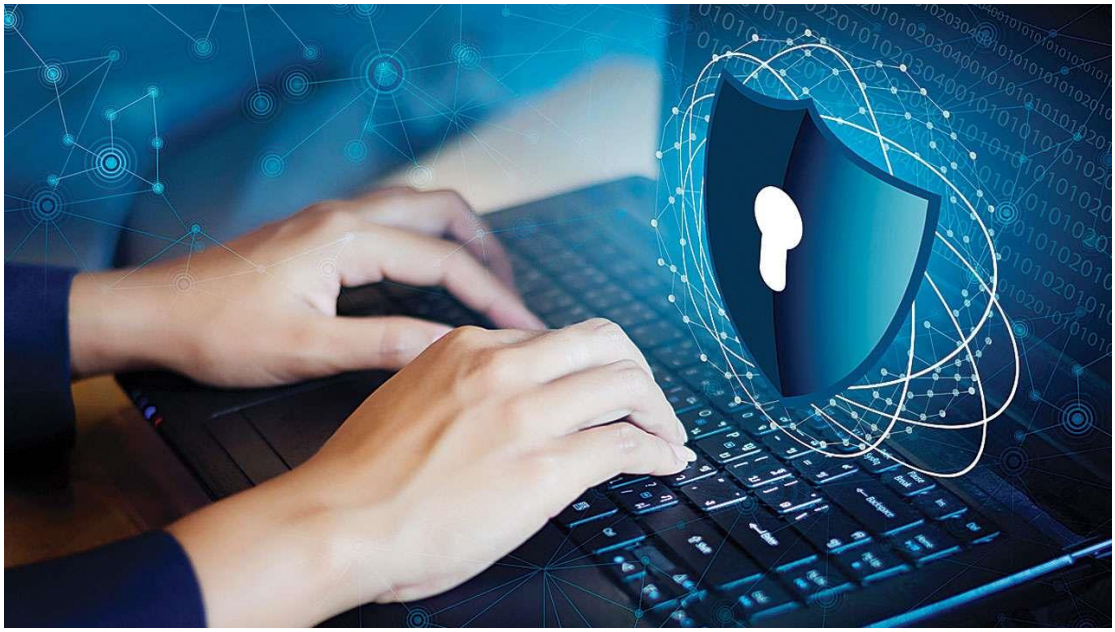
人无信不立，业无信不兴，国无信不强。诚信是公众必须具备的基本素养，也是文明社会不可或缺的基石。进入信息时代，快速发展的信息技术让人们生产生活更便捷、通信交流更畅通、信息获取更方便，但也带来了不同形式、不同程度的诚信缺失问题。信息时代呼唤诚信，迫切需要让诚实守信成为全社会的高度共识和行为自觉。

进入信息时代，智能手机、移动互联网、在线社交软件等日益普及，大数据、云计算、物联网、人工智能、区块链等新兴科技快速发展。截至 2018 年底，我国网民规模达到 8.29 亿，互联网普及率达到 59.6%。数字经济规模达到 31 万亿元，约占国内生产总值的 1/3。《数字中国建设发展报告（2018 年）》显示，2018 年 31 个省市区信息化发展指数平均达到 67.15%，比上年提升 4.88%。借助信息技术，人们在家中指尖轻点就可远程购物、远程学习、远程就医，“互联网+政务服务”让社会治理更加智能化、精准化、科学化。从迭出爆款的新媒体到热点不断的网络综艺，从如火如荼的电子商务到改变生活的共享经济，信息技术正在为社会生活带来越来越多的精彩和便利。

但也要看到，同其他新技术一样，信息技术具有明显的双刃剑效应，正当使用带来的是便利，不正当使用则会造成严重的伦理风险，这其中就包括诚信缺失问题。例如，利用信息技术，一些不法分子盗用他人社交账号诈骗钱财；极少数商家通过疯狂刷单来伪造好评；少数新媒体一味求快，未经调查核实就发布信息，导致新闻时有“反转”；等等。出现这些问题，一方面表明在信息时代少数人诚实守信的“螺丝帽”拧得还不够紧，另一方面反映出社会诚信建设仍存在一些亟须补齐的短板。

信息时代之所以出现诚信缺失问题，主要有以下几方面原因：

从技术层面看，信息技术具有数字化、虚拟化、开放性等特点，借助信息技术，人与人之间的交流更多呈现符号化、超地域性、隐匿性等特征。这让人际交往似乎进入一个互不熟识、缺少监督的“陌生人社会”，从而使一些人放松或忽视了诚信自律，做出失信行为。从利益驱动层面看，少数门户网站、自媒体重经济效益轻社会效益，为最大程度攫取经济利益不惜当“标题党”，甚至传递虚假信息，恶意透支社会信用。从体制机制层面看，相较于快速更新迭代的信息技术，诚信监督体系建设比较滞后，对失信者的威慑和惩戒还不够及时、有力，甚至在个别领域存在“牛栏关猫”的现象，从而让失信者有机可乘，造成诚信缺失问题。



中华优秀传统文化历来具有讲诚信、重承诺的优良传统。我们党一贯高度重视诚信建设，将诚信作为社会主义核心价值观的重要内容之一，把说老实话、办老实事、做老实人作为立身做人、干事创业的基本准则。“人而无信，不知其可也”。如果听任诚信缺失现象蔓延，不仅会带来社会信息交流不畅，而且会导致人与人之间缺乏必要的信任感，甚至会出现信任危机。

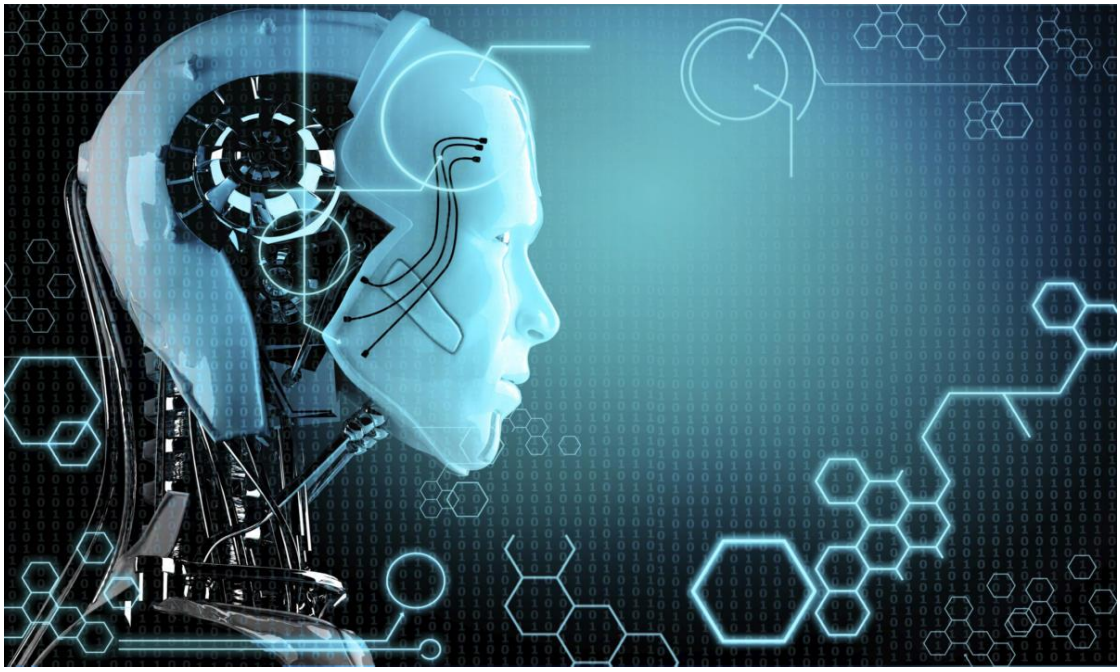
在信息技术快速发展的当下，有效提升公众诚信意识和社会信用水平，关键是加强网络诚信建设，坚持法治与德治并举、线上与线下联动，推动网络诚信建设法规越来越严密、覆盖越来越广泛、要求越来越严格。要在不断完善顶层设计、解决突出问题、形成长效机制上下功夫，打好网络诚信建设“组合拳”，综合运用互联网、大数据、云计算、人工智能等信息技术手段，广泛发动公众监督举报网上失信行为，开展诚信等级评价，动态发布诚实守信

“光荣榜”和失信者“黑名单”，让诚实守信者受到尊重，令失信违约者处处受限，在人人参与、多元共治中大力营造诚实守信的健康网络生态。（来源：人民网 孙伟平上海大学社会科学学部主任、马克思主义学院院长）

➢ 人工智能“脆弱面”暗藏安全风险

智能机器人自信地“走上”舞台担纲主持；无人车在测试道路上完成一系列动作，司机却稳坐千里之外；智能健康“魔镜”能实时显示测试者“睡眠”“情绪”“皮肤”等一系列健康指标系数……曾经在科幻电影中才能看到的炫酷片段已经在生活中得以实现，种种“黑科技”被广泛应用，人工智能的发展深刻地影响着社会生活。

但同时，随着人工智能技术应用越来越广泛，人工智能“脆弱面”也逐渐暴露，机器人“自我意识”、技术滥用等安全漏洞引起业界更多关注。专家表示，要加强对潜在风险的研判和防范，确保人工智能各项技术安全、可靠、可控。



催生新攻击方式

当今，世界各国纷纷布局人工智能，国际竞争日趋激烈。然而，人工智能的快速发展也使得网络安全的风险点和攻击方式出现新变化，进而引发更深层次的网络安全风险。

2018 年 4 月，欧盟委员会计划 2018 年至 2020 年在人工智能领域投资 240 亿美元。2018 年 5 月，法国发布《法国人工智能战略》，目的是使法国成为人工智能强国。2018 年 6 月，日本《未来投资战略》重点推动物联网建设和人工智能的应用。

对于人工智能，我国同样高度重视。2017 年，政府先后发布了《新一代人工智能发展规划》和《促进新一代人工智能产业发展三年行动计划（2018—2020 年）》。

北京邮电大学教授李小勇表示，我国是受到网络攻击最严重的国家之一，也是遭受物联网攻击最严重的国家之一，网络攻击手段和攻击形式越来越多。从行业来看，经济、教育、政府等部门成为攻击的主要目标。

360 公司董事长兼 CEO 周鸿祎说，网络攻击每天都在发生。目前网络黑客的攻击目标非常明确，就是能源、交通等基础设施，因为这样产生的影响是最大的。未来在万物互联的情况下，每个集装箱、每辆卡车，甚至城市里的每个井盖都实现互联，虚拟层面的攻击可能引发物理空间的损害。

事实上，劫持智能设备已经成为网络攻击的重要手段。网络安全专家表示，许多无人值守系统运用人工智能技术，一旦遭网络劫持，将带来严重的安全问题。例如，智能汽车可与车厂服务器连接，通过手机远程控制，车主需要定期更新软件保证汽车的驾驶模式，如此一来就可能被网络劫持。

天津大学法学院院长孙佑海称，网络攻击者可通过漏洞控制人工智能算法，实现物理硬件操纵、实施舆论引导、制造虚假图像或影响、制造信息噪音等，造成安全隐患。

此外，图像、声音合成滋生新的风险。国家互联网应急中心的相关专家称，随着技术的发展，现在的合成图像、语音越来越逼真。如果把该技术用于网络诈骗，虚构人脸和语音，是非常可怕的事情。

暴露安全软肋

由于人工智能技术依托的算法、大数据等可以很低的成本进行复制和扩散，其传播渠道广，监管难度大，封控几率低。

目前，人工智能技术正由“弱人工智能”向“强人工智能”阶段跃进，能够依据其所掌握的算法、数据，在短时间内快速突破人类传承多年的经验积累。

2016 年，由谷歌旗下“深度思维”（DeepMind）公司开发的 AlphaGo 横空出世，经深度学习后横扫人类围棋界翘楚。一年后，零基础起步的新程序 AlphaGo Zero，通过自我训练，在三天内与自身对弈 490 万局后，以 100：0 的成绩击败“前辈”AlphaGo。

2017 年，美国社交媒体平台脸书公司实验室中的两个人工智能机器人使用机器学习相互对话，并不断进行对话策略迭代升级，逐渐发展出了一种机器之间能理解但人类无法理解的语言。

“事实表明，人工智能通过算法和大数据进行深度学习，不排除演化出‘自我意识’的

可能，辅助甚至代替人类做出分析和决策，这易于发生反噬风险。”孙佑海说。

当前，人工智能研究高度开放附带源代码的海量论文可免费下载，即便编写一种折型算法的时间成本也只需几天，人工智能技术的滥用风险激增。此外，人工智能既有多学科综合、高度复杂等特性，带有天然的技术壁垒，给监管部门的监督管理和风险防范提出了不小的挑战。

除技术发展外，人工智能带来的社会影响不容小觑。通过特定算法全方位了解用户偏好和需求，为消费者“量身定制”的“精准推送”正成为商家引导消费的新途径。

近年来，北京、上海、重庆、济南等地的商圈开始试水“智慧商圈”模式，可以根据顾客的特征更精准地推送优惠券商品信息，让用户更有消费动力。比如，给年轻的未婚白领女性推送化妆品和奢侈品的品牌商券；给妈妈们推荐婴儿用品店；给男性推送运动品牌门店活动，等等。

“智慧商圈”带来生活便捷却容易引发“信息骚扰”问题。消费者的一个简单操作就有可能暴露想要购买某件商品的想法，后续会不断收到同类商品的广告宣传，产生困扰。长此以往，商场导购等从事决策分析、艺术创作等工作也有被机器人取代的可能，人工智能技术的日臻成熟将打碎传统职业群体的“饭碗”，进而引发新产业革命和经济结构调整，形成“去劳动力”倾向，最终产生失业风险。

不仅如此，人工智能产生的道德伦理隐忧不断。有专家表示，人工智能设计者的价值导向和行为偏好易于被有意或无意地反映到算法、数据当中，并通过机器学习被人工智能所承继，进而演进为算法歧视。而在具体适用过程中，容易受到对抗样本的干扰或污染，被应用

者二次形塑，做出背离设计初衷的错误决策。

2016 年 3 月，美国微软公司发布了名为 Tay 的最新版本人工智能机器人。然而，上线不到 24 小时，Tay 就“学坏”了：出言不逊、脏话不断，言语甚至涉及种族主义、色情、纳粹，充满歧视、仇恨和偏见。微软只得不停删除 Tay 的不当言论，进行下线调整。

用好“双刃剑”

专家表示，在人工智能飞速发展的时代，安全问题日益凸显，需要我们加强对潜在风险的研判和防范，切实维护好人民利益和国家安全，确保人工智能安全可靠、可控。

南开大学周恩来政府管理学院教授吴晓林认为，数字化、网络化、智能化已经是时代的主题，智能让生活变得更美好，但安全问题无处不在、无时不在。互联网下半场是工业互联网，以后国家的基础设施安全、工业互联网安全非常关键，还是要把人工智能的双刃剑用好，趋利避害，让科技的智能与人类的智慧并存、和谐。

在网络安全防护上，应加强技术研究，建立有效安全防护，抵御网络攻击。专家建议，可以建立主动免疫的计算架构，对计算进行安全防护，使计算全程可测可控，不被干扰。利用人工智能应对网络攻击，“免疫系统”中不管哪个系统受到攻击，都有统一的人工智能系统发出指令，采取相应措施。

在法治建设保障上，中国法学会副会长兼秘书长张鸣起建议高度重视立法工作，适时安排宏观立法，人工智能的发展离不开一部反映时代需求的《人工智能法》以及配套法规组成的法律法规体系。

孙佑海建议，全国人大宜进行立法上的一些准备，建议有关部门优先对无人机的管理、自动驾驶、图像识别相对成熟的技术应用制定法律规章，以刚性的法规条款引领秩序。

同时，要进一步健全精准务实的政策支撑体系，构建政策集群。孙佑海说，要进一步升级全流程的安全防控体系，并制定行业安全标准，做好应急防范的预案，加大重点领域的防控，加大对代码数据、算法等重点领域的综合管控力度，保障技术安全、产品安全、数据安全和应用安全。

针对新一代人工智能可能引发的结构性失业等风险，吴晓林建议，由劳动部门牵头加强与人工智能产业需求配套的在职培训和再就业培训体系，打好劳动力转型的主动仗。（来源：经济参考报）

➢ 国家互联网应急中心：我国云平台安全风险较为突出

国家互联网应急中心 17 日在此间发布的《2018 年中国互联网网络安全报告》显示，云平台成为发生网络攻击的重灾区，云服务商和云用户应加大对网络安全的重视和投入，分工协作提升网络安全防范能力。

据报告统计，在各类型网络安全事件中，云平台上的分布式拒绝服务攻击(DDoS 攻击)次数、被植入后门的网站数量、被篡改的网站数量占比均超过 50%。同时，国内主流云平台上承载的恶意程序种类数量占境内互联网上承载的恶意程序种类数量的 53.7%，木马和僵尸网络恶意程序控制端 IP 地址数量占境内全部恶意程序控制端 IP 地址数量的 59%，表明攻击者经常利用云平台来发起网络攻击。

据介绍，2018 年，国家互联网应急中心共协调处置网络安全事件 10.6 万起，其中网页仿冒事件最多，接下来依次是安全漏洞、恶意程序、网页篡改、网站后门、DDoS 攻击等。去年全年国家互联网应急中心成功切断了黑客对境内约 390 万台感染主机的控制。

报告显示，由于党政机关和重要行业加强了网络安全防护措施，去年针对这些机构的网络安全事件大幅减少，遭植入后门的政府网站数量平均减少了 46.5%。

报告还指出，随着移动互联网技术的快速发展和应用普及，2018 年通过移动应用实施网络诈骗的事件较为突出，如大量虚假的“贷款 App”被诈骗分子用于骗取用户隐私信息和

钱财。另外还有大量仿冒 App 采用“蹭热度”等方式传播和诱导用户下载安装，带来用户个人隐私信息泄露和恶意扣费等危害。

报告同时提醒，随着我国 5G、IPv6、物联网等试用工作逐步推进，新技术、新应用带来的安全问题需要提早加以关注和防范。（来源：国家计算机网络应急技术处理协调中心）

- **2018 年中国互联网网络安全报告**
- **全文：**https://www.cert.org.cn/publish/main/upload/File/2018annual.pdf

➢ 隐私保护的“中国方案”该如何完善

近日，全国信息安全标准化技术委员会、中国消费者协会等部门成立 App 专项治理工作组，对用户数量大、与民众生活密切相关的 App 隐私政策和个人信息收集使用情况进行评估并通报。通报称，中国银行手机银行等 10 款 App 无隐私政策；趣店、探探等 20 款 App 强制用户“一揽子”授权。

能否既玩消消乐又不让你读取我的通讯录？如果不提供地理位置读取授权，还能不能听首音乐……要么“信息裸奔”，要么“弃之不用”，面对 App 的默认勾选，用户如今依旧只能陷入被动的困境。进入数字时代以来，数据的重要性早已深入人心，“数字时代的石油”成为大家对数据的共识。互联网企业广泛收集用户各类信息加以整理分析利用，从中攫取到巨大的经济效益。在这过程中，暴露出的个人数据安全、隐私保护等问题却被忽视。随着欧盟《一般数据保护条例》（GDPR）的生效，欧洲范围内建立起了一套在隐私管理、个人信息安全保护和数据流动之间的复合机制。GDPR 之后，越来越多的国家开始聚焦自身隐私安全问题，中国也不例外。

如今，GDPR 已实施一年多，它的经验得失被广为讨论、借鉴，一些隐私保护的原则与技术创新的冲突也不断具像化。那么，隐私保护的“中国方案”该如何完善？

对 GDPR 的反思

GDPR 正式实施后，想进入欧洲市场的企业纷纷修改自身的隐私政策，并提升保护用户个人数据的技术手段，来避免受到严厉的惩罚，这在有力地保护了用户个人数据的同时，客观上也加大了企业的成本支出。

在诸多对 GDPR 的“吐槽”中，最集中的一项便是企业在合规方面的支出多了，会加重企业的负担。根据《福布斯》报告，GDPR 让美国财富 500 强企业多花费了 78 亿美元合规成

本。普华永道给出更明确的合规成本估计：68%的公司预计将花费 100 万到 1000 万美元。

在此环境下，企业面临的生存压力不小。此前，在“2019 罗汉堂数字经济年会”上，多位专家对此议题展开了讨论。国际数据隐私实践联合主管，Bird&Bird 合伙人阿里安娜·默勒说，小型企业对于未来的发展充满矛盾：一方面，他们需要通过遵守 GDPR 获取客户的信任；另一方面，遵守 GDPR 需要花费大量的资金，但事实上，“它们没有足够的资本”。

这一困扰引发社会对初创企业健康成长的担忧，诺奖学者、法国图卢兹大学产业经济研究所科研所长让·梯若尔正在反思这一结果，“我们不能因噎废食，个人隐私确实需要保护，但在保护个人隐私的同时，不能遏制科技的进步和创新的发展。”

看上去似乎是个两难的选择，一面是企业的成长和创新，一面是个人隐私的保护。有企业家进一步提出，数字时代想抹掉已经泄露的个人数据几乎是不可能的，个人的信息一旦被发布在网上，就会被互联网永远保留，那该如何按下“删除键”呢？

GDPR 为此规定了“被遗忘权”，该项权利主张数据主体有权要求控制者删除相关的个人数据。但对于“被遗忘权”的具体执行，仍存在许多问题。阿里安娜·默勒表示，被遗忘权实际上规定的就是数据的持有时期——“个人数据在使用之后，能够被合法地保留多久”。但对企业而言，执行起来仍然很困难。

阿里安娜·默勒说，企业要想合规，必须按照法律进行技术设计。但现实情况却是，法律规定自身就在不断地变化，“虽然出台这些法律规定的初衷是好的，但他们也要意识到，在不断地修改法规，或者对自己的法律法规不断给出解释的时候，并没有真正地帮到企业和个人。”

而在译言联合创始人赵嘉敏看来，人们当前想要拥有“删除键”的意识是基于隐私观念。

但现实情况是，隐私的概念本身就在不断演化。可持续性的解决方案也许不是去要求技术来遵从我们的传统习惯，而是要去改变我们的传统意识和社会规范，以更好地适应技术的发展，并让个体和群体都能从这种改变中受益。

完善“中国方案”

对于企业为合规而付出的高额成本，重庆大学国家网络空间安全与大数据法治战略研究院院长齐爱民表示，企业在 GDPR 正式实施初期，不可避免地要修改自身的隐私政策，在此过程中，企业需要支出较大的成本来达成这一任务目标。但是，只要企业的个人数据保护合规工作进入正轨，那么之后的维护成本也将大大降低，并不会过多地影响企业的技术创新问题。

“另外，由于 GDPR 的实施，提升了商业环境中对个人数据安全的保护，促成了针对隐私友好型创新的发展。换言之，隐私友好型的技术创新将成为下一个技术创新的基本模式。”齐爱民说。

法国国务顾问、法国数据保护局(CNIL)前副主席伊莎贝尔·法尔克·皮尔罗廷甚至直接反驳了“高额成本”的说法，“像法国数据保护局，他们就常开展一些教育培训，专门来辅导和教育初创企业如何做到隐私保护合规，从产品早期设计开始就考虑隐私的问题，那根本就没有多少成本。”无论细节上有多少差异，保护隐私已是共识。北京安理律师事务所高级合伙人王新锐曾表示，很多大型公司在做完 GDPR 合规后，透明度明显有提升，也给了用户更多选择。

事实上，我国正在快速推进隐私保护工作。去年，推荐性国家标准《信息安全技术个人

信息安全规范》（以下简称《规范》）正式实施。这部由 33 位拥有政策制定、技术标准、企业实践经验的专家共同起草，历经两年多博弈的《规范》对个人信息收集、保存、使用、流转等环节提出要求，非常明确地把《网络安全法》原则性的规定给落地了，填补了国内个人信息保护在实践标准上的空白。

但问题也很明显，《规范》是推荐性标准而非强制性标准，因此不具备法律强制力，在齐爱民看来，《规范》在对信息主体的个人信息保护力度上是远远不够的。“虽然我国关于个人信息保护的相关法规散见于《民法总则》、《网络安全法》、《电子商务法》和《消费者权益保护法》等相关立法文件中，但是我国尚未出台一部专门的《个人信息保护法》。”

王新锐说，下一步应该就是立法了，中国个人信息保护的立法者现在面临的是一方面要“补课”，借鉴各国立法中被证明有效的部分，另一方面又要回答中国的独特性问题，尤其是移动互联网高速发展带来的问题。“哪些可以借鉴国际规则，哪些必须要自己原创性的回答，这本身就是一个非常难的问题。”王新锐表示，现阶段立法还是应该以补课为主要目标，适度留有口子，而对于新型问题，可以先以位阶较低的规则加以应对，待成熟稳定后再上升为立法。

复旦大学网络空间治理研究中心主任沈逸也认为，当前我国可通过“小步快走”的方式逐步将法规上升为法律，“推出一些原则性的规定，然后迅速地把它细化，然后在细化和实践的过程中，如果发现有些东西和实践之间发生了比较大的冲突，再做及时的调整。”

在这方面，齐爱民认为，GDPR 的经验可供借鉴。GDPR 赋予信息主体强大的个人信息权利的同时，忽略了复杂多变的现实生活场景对个人信息的不同需求。“未来立法者可以考虑采用以《个人信息保护法》为主，授权相关主管部门制定该特定行业的个人信息保护配套规则的立法模式，更加灵活地处理不同场景对于个人信息的需求。”

除此之外，沈逸认为，各国在治理互联网隐私保护时，也应考虑到互联网跨国互通的这一属性，实现联合治理。

“把主权边界机械化地延伸到网络空间去，肯定是有问题的。”沈逸说，这极有可能将互联网“切得七零八落”。所以，使数据能在全球范围内流动和被管辖，制定一个既维护全球网络空间的稳定，又能让数据流动更有序的全球规范极为重要。

显然，这还有很长的路要走。正如罗汉堂秘书长、湖畔大学执行教育长陈龙所言，“所有的人都同意，一定的隐私保护是应该的，但当信息的交流同时成为这个时代的动力和种种担忧的源头，同时其中的取舍对每个人都不同的时候，应该怎么做？”在这个话题上，没有简单的理所当然。（来源：中国青年报）

四、政府之声

➢ 互联网信息服务投诉平台正式发布

2019 年 7 月 11 日，中国互联网协会在北京国家会议中心召开发布会，互联网信息服务投诉平台正式上线运行。工业和信息化部信息通信管理局副局长鲁春丛参加发布会。

互联网信息服务投诉平台是在工业和信息化部指导下，中国互联网协会建设运营的第三方投诉渠道，投诉平台坚持“以人民为中心”的发展思想，定位于“绿色通道”，旨在快速化解用户与企业之间的服务纠纷，是保护用户合法权益的重要途径，也是行业自律和社会监督的重要组成部分、政府监管的有力支撑。自 2019 年 4 月 8 日试运行开始，投诉平台充分发挥了桥梁作用，用户投诉得到及时处理，企业的快速响应有效提升了用户获得感。

不忘初心，方得始终。服务用户是建设投诉平台的初心，也是广大企业的初心。欢迎更多的互联网企业积极接入互联网信息服务投诉平台，快速响应用户合理诉求，切实保障用户合法权益。

中国信息通信研究院总工程师胡坚波及腾讯、百度、阿里巴巴、京东、美团、支付宝、字节跳动、唯品会、携程、新浪、新浪微博、爱奇艺、猎豹移动、苏宁易购、探探文化、中外法制网等 16 家接入平台企业代表参加发布仪式。（来源：工信部）

- **互联网信息服务投诉平台**

- **网址：**https://ts.isc.org.cn/

➢ 《加快推进社会信用体系建设构建以信用为基础的新型监管机制意见》印发

2019 年 7 月 16 日，国务院办公厅印发《关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》（以下简称《意见》）。

《意见》指出，要以习近平新时代中国特色社会主义思想为指导，按照依法依规、改革创新、协同共治的原则，以加强信用监管为着力点，创新监管理念、监管制度和监管方式，建立健全贯穿市场主体全生命周期，衔接事前、事中、事后全监管环节的新型监管机制，不断提升监管能力和水平，进一步规范市场秩序，优化营商环境，推动高质量发展。《意见》提出了四个方面政策措施。

一是创新事前环节信用监管。建立健全信用承诺制度，对申请人承诺符合审批条件并提交材料的有关行政许可事项应予即时办理，鼓励市场主体主动向社会作出信用承诺；充分利用各级各类政务服务窗口，探索开展经营者准入前诚信教育；积极拓展信用报告应用，鼓励各类市场主体在生产经营中更广泛、主动地应用信用报告。

二是加强事中环节信用监管。全面建立市场主体信用记录，及时、准确、全面记录市场主体信用行为，特别是将失信记录建档留痕，做到可查可核可溯；建立健全信用信息自愿注册机制，鼓励市场主体在“信用中国”网站或其他渠道上自愿注册信用信息；开展全覆盖、标准化、公益性的公共信用综合评价，为信用监管提供更精准的依据；大力推进信用分级分类监管，根据市场主体信用状况实施差异化监管措施。

三是完善事后环节信用监管。健全失信联合惩戒对象认定机制，督促失信市场主体限期整改，深入开展失信联合惩戒，坚决依法依规实施市场和行业禁入措施，依法追究违法失信责任，探索建立信用修复机制。

四是强化信用监管的支撑保障。提升信用监管信息化建设水平，形成信用监管协同机制；大力推进信用监管信息公开公示，做到“应公开、尽公开”；充分发挥“互联网+”、大数据对信用监管的支撑作用，实现信用监管数据可比对、过程可追溯、问题可监测；切实加大信用信息安全和市场主体权益保护力度，积极引导行业组织和信用服务机构协同监管。

《意见》要求，各地区各部门要加强组织领导，细化责任分工，加强与其他“放管服”改革事项的衔接，组织开展信用建设和信用监管试点示范。加快建章立制，推动制定社会信

用体系建设相关法律法规。通过各种渠道和形式，深入细致向市场主体做好政策宣传解读工作。（来源：国务院办公厅）

- **国务院办公厅《关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》国办发〔2019〕35 号**
- **全文：**http://www.gov.cn/zhengce/content/2019-07/16/content_5410120.htm

➢ 教育部、中央网信办等六部门发布《关于规范校外线上培训的实施意见》

2019 年 7 月 12 日，为规范面向中小学生、利用互联网技术实施的学科类校外线上培训活动（以下简称校外线上培训），促进其持续健康有序发展，切实减轻中小学生过重课外负担，教育部等六部门印发了《关于规范校外线上培训的实施意见》（以下简称《实施意见》）。

《实施意见》指出，坚持育人为本，推动校外线上培训遵循教育规律和学生身心发展规律，不断提高培训的科学性、规范性和适宜性；坚持依法规范，依法依规对校外线上培训进行监管，促进校外线上培训机构加强行业自律、有序开展培训业务；坚持协同治理，建立相关部门齐抓共管的工作机制，采取“互联网+监管”新模式，积极稳妥推进。

《实施意见》明确，2019 年 12 月底前完成对全国校外线上培训及机构的备案排查；2020 年 12 月底前基本建立全国统一、部门协同、上下联动的监管体系，基本形成政府科学监管、培训有序开展、学生自主选择的格局。

《实施意见》提出三方面的主要措施：一是实施备案审查制度。备案审查重点是培训机构、培训内容和培训人员；备案审查流程是：校外线上培训机构在取得 ICP 备案（涉及经营电信业务的，还应当申请电信业务经营许可）、网络安全等级保护定级备案的证明、等级测评报告后，向机构住所地的省级教育行政部门提交相关材料，申请备案。二是开展排查整改。省级教育行政部门会同网信、电信、公安、广电、“扫黄打非”等部门制订排查方案；排查监管的重点是内容健康、时长适宜、师资合格、信息安全、经营规范等方面情况； 2019 年 12 月底前完成排查，并对发现的问题限期整改，于 2020 年 6 月底前完成整改。三是健全监管机制。强化综合治理，探索“互联网+监管”机制，改进监管技术手段，建设全国校外线上培训管理服务平台；明确教育、网信、电信、公安、广电、“扫黄打非”等部门职责分工；建立黑白名单，及时更新，实现动态监管；加强行业自律，提高培训质量，提升培训对象满意度。

《实施意见》强调，各地要统筹校外线下和线上培训规范治理工作，在当地党委和政府的领导下建立教育部门牵头、有关部门参与的工作机制，制订详细的工作方案和应急预案；加强公共服务，强化问责考核，确保各项目标落实到位。（来源：教育部）

- **《教育部等六部门关于规范校外线上培训的实施意见》教基函〔2019〕8 号**
- **全文：**http://www.moe.gov.cn/srcsite/A06/s3325/201907/t20190715_390502.html

➢ 《儿童个人网络信息保护倡议书》发布

2019 年 7 月 18 日，由全国人大社会建设委员会和国务院妇女儿童工作委员会办公室指导，中国网络社会组织联合会和联合国儿童基金会联合主办的 2019 未成年人网络保护研讨会上，中国网络社会组织联合会副秘书长张勇代表大会发布《儿童个人网络信息保护倡议书》。

《儿童个人网络信息保护倡议书》全文：儿童是祖国的未来，儿童的健康成长是全社会的共同希望。随着信息技术快速发展，互联网已成为儿童求知、社交和娱乐的重要平台。为儿童构建良好的内容生态、提升儿童网络素养、维护儿童网络权益、保护儿童网络安全，对儿童的健康成长意义重大。

为此，中国网络社会组织联合会与联合国儿童基金会共同主办 2019 未成年人网络保护研讨会，邀请政府、社会组织、企业、学校的代表及部分家长和儿童代表，共同就加强儿童

个人网络信息保护，为儿童营造健康的网络环境进行研讨交流，并发出如下倡议：

一、社会各界应当充分尊重儿童平等、正确、合理使用网络的权利，共同致力于促进儿童全面健康成长。

二、政府主管部门应当依法依规积极开展儿童个人网络信息保护工作，建立政府主导、社会参与的工作机制，及时处理侵犯涉及儿童个人信息的违法违规行为。

三、各类组织和个人应当尊重和保护儿童的网络隐私权，不得在网络上非法收集、存储、使用、转移、披露和传播儿童个人信息。

四、网络社会组织应当积极督促并协助互联网企业加强行业自律，履行社会责任，推动制定儿童个人网络信息保护的行业规范和行为准则。

五、互联网企业应当切实履行儿童个人网络信息保护的平台责任，严格依照法律规定和用户协议收集和使用儿童个人信息。严格遵守必要性原则，收集、使用和转移儿童个人信息应征得儿童父母或者其他监护人同意；尊重儿童个人网络信息的删除权，对儿童及其监护人提出的删除儿童网上个人信息的诉求，应依法依规予以配合。

六、学校应当加强儿童网络素养教育，开设专门课程，引导儿童正确上网用网，提高儿童对个人网络信息的自我保护能力。

七、家庭在儿童养成良好上网习惯中发挥着最重要的作用，儿童的父母或者其他监护人应当履行法定监护责任，做好表率，加强教育，确保儿童正确、合理使用互联网。

八、儿童应当主动提高个人信息保护意识，上网时不随意泄漏个人和他人信息，遇到填写个人隐私内容的要求，应当主动征询父母或者其他监护人，做到依法上网、理性上网、文明上网。（来源：网络传播杂志）

五、本期重要漏洞实例

➢ 关于 Redis 存在远程命令执行漏洞的安全公告

发布日期：2019-07-10

描述：2019 年 7 月 10 日，国家信息安全漏洞共享平台（CNVD）收录了 Redis 远程命令执行漏洞（CNVD-2019-21763）。攻击者利用该漏洞，可在未授权访问 Redis 的情况下执行任意代码，获取目标服务器权限。目前，漏洞利用原理已公开，官方补丁尚未发布。

漏洞情况分析：

Redis 是一个开源的使用 ANSI C 语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value 数据库，并提供多种语言的 API。作为一个高性能的 key-value 数据库，Redis 在部分场景下对关系数据库起到很好的补充作用。

2019 年 7 月 7 日，LC/BC 的成员 Pavel Toporkov 在 WCTF2019 Final 分享会上介绍了 Redis 新版本的远程命令执行漏洞的利用方式。由于在 Reids 4.x 及以上版本中新增了模块功能，攻击者可通过外部拓展，在 Redis 中实现一个新的 Redis 命令。攻击者可以利用该功能引入模块，在未授权访问的情况下使被攻击服务器加载恶意.so 文件，从而实现远程代码执行。

CNVD 对该漏洞的综合评级为“高危”。

漏洞影响范围

漏洞影响的产品版本包括：

Redis 2.x，3.x，4.x，5.x

*>

建议：

目前，Redis 官方暂未发布补丁，临时解决方案如下：

1、禁止外部访问 Redis 服务端口；

2、禁止使用 root 权限启动 Redis 服务；

3、配置安全组，限制可连接 Redis 服务器的 IP。

建议使用 Redis 数据库的信息系统运营者进行自查，发现存在漏洞后，按照临时解决方案及时进行修复。

附：参考链接：

https://paper.seebug.org/975/

➢ Cisco Webex Business Suite 安全绕过漏洞

发布日期：2019-07-15

更新日期：2019-07-15

受影响系统：

Cisco WebEx Business Suite

描述：

BUGTRAQ ID: 106939

CVE(CAN) ID: CVE-2019-1680

Cisco Webex Business Suite 是美国 Cisco 公司的一套视频会议解决方案。

Cisco Webex Business Suite 3.0.9 之前版本中存在安全绕过漏洞，该漏洞源于不合理输入验证。未经验证的远程攻击者可利用该漏洞通过诱导目标用户查看恶意 URL 将任意文本注入用户的浏览器并根据注入的文本内容实施欺骗攻击。

<*来源：Prasenjit Kanti Paul

链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-webex-inject

*>

建议：

厂商补丁：

Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190206-webex-injection）以及相应补丁:

cisco-sa-20190206-webex-injection : Cisco Webex Meetings Online Content Injection Vulnerability

链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-webex-inject

➢ 多个 SAP 产品远程授权绕过漏洞

发布日期：2019-07-11

更新日期：2019-07-11

受影响系统：

SAP HANA Financial Products Subledger 1

SAP FSAPPL 5

SAP Banking services 9.0

描述：

BUGTRAQ ID: 107353

CVE(CAN) ID: CVE-2019-0276

SAP HANA Financial Products Subledger 是德国 SAP 公司开发的一款针对银行、保险和再保险公司、金融科技公司和其他公司金融产品的综合平台。SAP FSAPPL，即 SAP Banking services 是德国 SAP 公司研发的一款面向消费者和商业银行的全面的，随时可运行的高级银行服务平台。

多个 SAP 产品中存在远程授权绕过漏洞，该漏洞源于 SAP 9.0 (FSAPPL 版本 5)中的银行服务和 SAP S/4HANA Financial Products Subledger (S4FPSL, version 1) 未对已认证用户执行充分的授权检查，攻击者可利用该漏洞获取敏感信息，导致权限升级。

<*来源：SAP

链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=515408080

*>

建议：

厂商补丁：
SAP

SAP 已经为此发布了一个安全公告（CVE-2019-0276）以及相应补丁：
CVE-2019-0276：SAP Security Patch Day – March 2019
链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=515408080

➢ IBM WebSphere MQ 跨站脚本执行漏洞

发布日期：2019-07-11
更新日期：2019-07-11
受影响系统：
IBM WebSphere MQ 9.1.0.1
IBM WebSphere MQ 9.1.0.0
IBM WebSphere MQ 9.0.5
IBM WebSphere MQ 9.0.4
IBM WebSphere MQ 9.0.3
IBM WebSphere MQ 9.0.2
不受影响系统：
IBM WebSphere MQ 9.1.1
描述：

BUGTRAQ ID: 107530
CVE(CAN) ID: CVE-2018-1836
IBM WebSphere MQ 是美国 IBM 公司的一款消息传递中间件产品。该产品主要为面向服务的体系结构提供可靠的、经过验证的消息传递主干网。
IBM WebSphere MQ 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.1.0.0, 和 9.1.0.1 版本中存在跨站脚本执行漏洞，该漏洞源于允许用户在 Web UI 中嵌入任意 JavaScript 代码，攻击者可利用该漏洞更改预期功能，导致可信会话中的凭据泄露。
<*来源：IBM （ncsupp@ca.ibm.com）
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10734457
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（150661）以及相应补丁：
150661：Security Bulletin: IBM MQ Console has inadequate input validation (CVE-2018-1836)
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10734457

六、本期网络安全事件

➢ K12.com 暴露了多达 700 万条涉及学生个人信息的数据库记录

2019 年 7 月 14 日，据 Comparitech 的安全研究人员称，在线教育平台 K12.com 本周无意中暴露了近 700 万学生的个人信息。暴露的数据库包含全名，电子邮件地址，出生日期和性别身份，以及学生就读的学校，同时还可访问其帐户的身份验证密钥和其他内部数据。

这些信息在线提供了一个多星期，目前还不清楚数据库是否被恶意行为者访问或者获取。据发现数据暴露的研究人员称，该问题影响了 K12.com 的 A+nyWhere 学习系统（A + LS），该系统被美国 1100 多个学区使用。

数据库配置错误可能是导致它可以在 BinaryEdge 和 Shodan 上公开访问和发现的原因，这两个搜索引擎专门为面向公众的数据库编制索引。 6 月 25 日发现的曝光首次发生在 6 月 23 日，直到 7 月 1 日才得以修复。

错误配置的数据库暴露公司收集和持有的大量个人信息的事件近年来变得非常普遍。就在最近几个月，面向公众的数据库暴露了大量 Instagram 知名人士账号的联系信息、康复病人的医疗记录、AMC Networks 高级服务的订户等等。在其中一个例子中竟然还发现了包含美国 8000 多万家庭敏感信息的数据库。在这种情况下，确实很难确定是否有人恶意访问了这些信息。（来源：cnBeta）

➢ 国泰君安员工窃取个人信息 400 万条 "超级黑客"被判 5 年

2019 年 7 月 15 日，国裁判文书网披露的《林清金非法获取计算机信息系统数据、非法控制计算机信息系统二审刑事判决书》显示，林清金是国泰君安证券经纪人，2018 年 7 月 20 日，福建省福州市中级人民法院终审判决林清金犯非法侵入计算机系统罪，判处有期徒刑七个月;犯侵犯公民个人信息罪，判处有期徒刑五年，并处罚金人民币二万元，数罪并罚，决定执行有期徒刑五年二个月，并处罚金人民币二万元。

判决书显示，林清金于 2017 年 1 月至 3 月，先后破解密码登入兴业证券系统主页，冒充兴业证券董事长兰某等人身份进入兴业证券的 OA 办公系统、VPN 系统;进入国有资产监督管理委员会、国家工商行政管理总局、阜阳市政府等多家国家事务机关网站;非法侵入长江证券的公司客户管理系统、OA 办公系统;非法侵入国泰君安、中信建投期货、中航期货的计算机系统。林清金侵入证券公司等机构的计算机系统非法获取公民个人信息共计 400 余万条。

国泰君安员工侵入 3 券商 2 期货公司计算机系统、改国家事务机关网站员工邮箱密码

判决书显示，林清金系国泰君安证券股份有限公司经纪人。福州市鼓楼区人民检察院指控原审被告人林清金犯非法侵入计算机系统罪、非法获取计算机信息系统数据罪、侵犯公民个人信息罪一案，于 2017 年 12 月 21 日作出(2017)闽 0102 刑初 1019 号刑事判决。

原审被告人林清金不服，提出上诉。林清金上诉称，其是为了提醒有关国家机关及证券交易公司注意弱密码问题，加强网络安全建设而实施侵入计算机等行为;其所获取的证券公司员工账号和密码不属于证券交易网络金融服务的身份认证信息，原判量刑过重，请求二审

法院从轻处罚。

经二审审理查明：2017 年 2 月 26 日至 2017 年 3 月 6 日，上诉人林清金在福建省泉州市丰泽区内多次利用自己所掌握的计算机知识、技术，破解密码登入兴业证券股份有限公司系统主页，后冒充兴业证券股份有限公司董事长兰某,信息技术部林某等人身份进入兴业证券股份有限公司的 OA 办公系统、VPN 系统，获取该公司员工身份认证信息 14 组，并下载导出公司员工通讯录及个人信息数据共 5963 组。

2017 年 1 月 12 日和 2 月 20 日，上诉人林清金在上述地点使用上述相同的作案手段进入国有资产监督管理委员会、国家工商行政管理总局、阜阳市政府等多家国家事务机关网站，非法侵入相关工作人员的邮箱，并修改了密码。

2017 年 2 月 26 日至 2017 年 3 月 6 日，上诉人林清金使用上述相同的作案手段，非法侵入长江证券股份有限公司的公司客户管理系统、OA 办公系统，下载客户姓名和电话的真实信息 3057191 条。

2017 年 2 月 26 日至 2017 年 3 月 6 日，上诉人林清金使用上述相同的作案手段，非法侵入国泰君安股份有限公司的计算机系统，下载信息共计 843821 条(包括姓名、手机号码、联系地址、计算所得总资产),国泰君安股份有限公司代理子公司期货公司开户客户数据 57287 条。

2017 年 2 月 26 日至 2017 年 3 月 6 日，上诉人林清金使用上述相同的作案手段，非法侵入中信建投期货有限公司的计算机系统，下载客户信息 82219 条(含：客户姓名、客户交易账号、客户银行账号、客户身份证号码、客户联系电话、客户地址);客户资产信息 82219 条(含：客户权益、成交金额、手续费、盈亏情况、成交手数、成交品种);员工信息 1081 条(含：员工编号、员工姓名、员工岗位)。

2017 年 2 月 26 日至 2017 年 3 月 6 日，上诉人林清金使用上述相同的作案手段，非法侵入中航期货有限公司的计算机系统，下载客户资料 14482 条(含：客户全称、证件号码、地址、电话、手机、指令下达人 123、指令下达人身份证号 123、资金调拨人 12、资金调拨人身份证号 12 等)。上诉人林清金于 2017 年 3 月 15 日被公安民警抓获。

非法获取个人信息 400 余万条 判刑 5 年 2 个月

福建省福州市中级人民法院认为，上诉人林清金违反国家规定，侵入国家事务领域的计算机信息系统，并侵入证券公司等机构的计算机系统非法获取公民个人信息共计 400 余万条，情节特别严重，其行为已构成非法侵入计算机系统罪、侵犯公民个人信息罪，应实行数罪并罚。上诉人林清金到案后如实供述自己的罪行，依法予以从轻处罚，辩护人的相关辩护

意见，予以采纳。关于林清金及其辩护人提出林清金具有投案行为，构成自首情节的诉辩意见，没有证据证实，不予采纳。原判认定上诉人林清金某成非法获取计算机信息系统数据罪，并以非法侵入计算机系统罪、非法获取计算机信息系统数据罪、侵犯公民个人信息罪，对上诉人林清金进行数罪并罚不当，属适用法律错误。

据此，福建省福州市中级人民法院依照《中华人民共和国刑法》、《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》、《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》及《中华人民共和国刑事诉讼法》的相关条款之规定，判决如下：

一、维持福建省福州市鼓楼区人民法院(2017)闽 0102 刑初 1019 号刑事判决第二项，即扣押在案的作案工具台式电脑主机两台、三星牌手机一部予以没收，由扣押单位负责执行。

二、撤销福建省福州市鼓楼区人民法院(2017)闽 0102 刑初 1019 号刑事判决第一项，即被告人林清金犯非法侵入计算机系统罪，判处有期徒刑七个月，犯非法获取计算机信息系统数据罪，判处有期徒刑七个月，并处罚金人民币二千元，犯侵犯公民个人信息罪，判处有期徒刑五年，并处罚金人民币二万元，数罪并罚，决定执行有期徒刑六年，并处罚金人民币二万二千元。

三、上诉人林清金犯非法侵入计算机系统罪，判处有期徒刑七个月;犯侵犯公民个人信息罪，判处有期徒刑五年，并处罚金人民币二万元，数罪并罚，决定执行有期徒刑五年二个月，并处罚金人民币二万元。

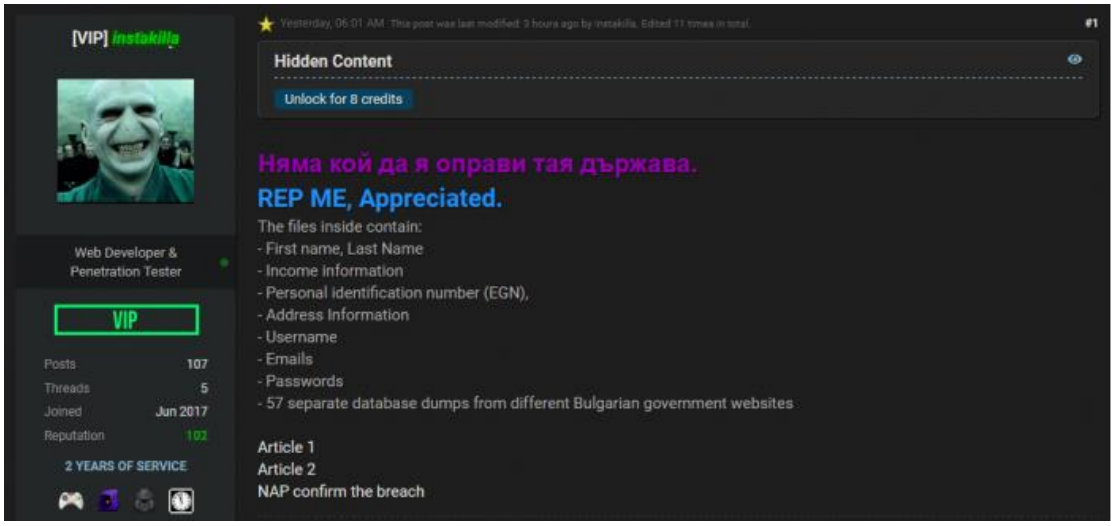
刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2017 年 3 月 16 日起至 2022 年 5 月 15 日止。罚金于判决生效后一个月内缴纳。)(来源：中国经济网)

➢ 举国无隐私！保加利亚遭黑客入侵 500 万民众信息外泄

2019 年 7 月 19 日，保加利亚国家税务局数据库被黑客攻破，高达 500 万国民的信息外泄——受害者总数相当于该国所有成年公民的总和，创下该国历史上最为严重的用户数据泄露事故。截至目前，一名年仅 20 岁的嫌犯已经落网，黑客团体及其作案动机正在进一步调查当中。

据英国路透社 17 日报道，保加利亚新闻媒体 15 日收到神秘电邮，自称是“俄罗斯黑

客”的寄信人号称攻破了该国官方 110 个数据库，其中包含核心政府部门的高度涉密信息。作案团伙在信中大肆嘲弄保加利亚当局的“腐败无能”，挑衅称“贵国的网络安全就是个笑话”。他们号称为媒体提供的数据包约为 11GB，他们手中还掌控着 10GB 左右的数据。保加利亚《24 小时报》称，这份邮件中包含部分失窃数据的下载链接，点击后可查看到 110 万公民个人关键信息，包括身份证、社保号码、个人收入、缴税记录以及医疗信息等。



保加利亚财政部方面证实，这起史无前例的网络入侵事件发生在上月底，该国国家税务局(NRA)的网络系统“失守”。税务部门官员表示，黑客团体的作案地点疑似位于境外，而黑客所发送的邮件也能追溯到俄罗斯。本月 16 日，国家税务局在一场新闻发布会上表示，黑客利用了该机构在线增值税退税服务的漏洞，大约窃取了 NRA 总数据量的 3%。保加利亚财政部长戈拉诺夫在国家议会上向全体公民道歉，不过他同时辩解称，外泄数据并非涉密信息，国家财政稳定性也不会被危及。因这起事故，国税局方面将面临 2000 万欧元的重罚。

据保加利亚通讯社 17 日报道，本月 15 日，一名年仅 20 岁的嫌疑人在该国普罗夫迪夫市落网。据起底，嫌犯名叫博科夫，是该国一家网络安全公司的程序员。据了解，此人在业内算是个“知名人士”，2017 年他曾因指出教育部官网的安全漏洞而名声大噪。如今，沦为阶下囚的博科夫或将面临 5 年至 8 年刑期以及 1 万列弗(约合人民币 4 万元)罚款。保加利亚警方表示，目前该案件的调查工作尚处于早期阶段，警方还在搜寻其他涉案嫌疑人。

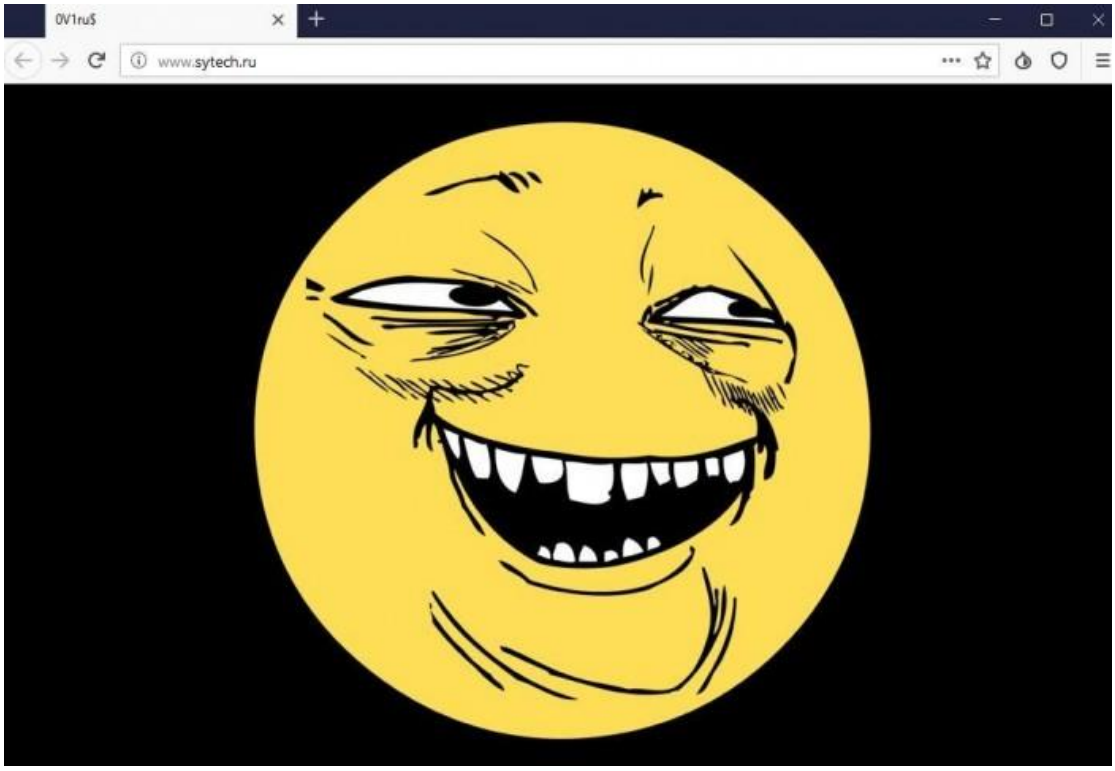
也许是为了挽救政府颜面，保加利亚总理鲍里索夫在 17 日的一场政府会议上称赞落网嫌犯是一名“奇才”，还表示这样的人物应该为国效力。但很快有网络专家表示，黑客所采用的侵入方式并不高明，只是数据库的保护措施太糟糕。虽然作案动机尚不明确，但不少媒体猜测黑客的目的是为了给政府“上一课”、是“白帽黑客”行为(指黑客通过入侵系统来检测网络安全性)，旨在刺激当局引入更有力的网络安全措施。也有美国媒体认为，这起大规

模网络攻击事件带有国际政治背景，暗示俄罗斯在“报复”保加利亚斥巨资购买美国的 F-16 战斗机。（来源：环球日报）

➢ 黑客攻入俄罗斯联邦安全局承包商服务器窃取 7.5TB 的数据

2019 年 7 月 21 日，黑客入侵了俄罗斯国家情报部门 FSB 的承包商 SyTech，并从那里窃取了该公司为 FSB 工作的内部项目的信息 - 包括用于对 Tor 流量进行去匿名化的信息。攻击事件发生在上周末，即 7 月 13 日，一群名为 0v1ru $的黑客入侵了 SyTech 的活动目录服务器，从那里他们获得了访问该公司整个 IT 网络的权限，包括一个 JIRA 实例。

黑客从承包商的网络中窃取了 7.5TB 的数据，末了他们还顺手用一个“yoba face”破坏了该公司的网站，这是一个受俄罗斯用户欢迎的表情符号。



黑客在 Twitter 上发布了该公司服务器数据的截图，后来又与数字革命组织分享了被盗数据。数字革命是另一个黑客组织，他们去年攻破了另一家 FSB 承包商 Quantum 公司。黑客组织之后还与俄罗斯记者在 Twitter 账户上更详细地分享了被盗文件。

根据俄罗斯媒体的报道，这些文件表明，自 2009 年以来，SyTech 已经为 FSB 和同行承包商 Quantum 开展了多个项目。项目包括：

Nautilus - 一个收集社交媒体用户（如 Facebook，MySpace 和 LinkedIn）数据的项目。

Nautilus-S - 在流氓 Tor 服务器的帮助下对 Tor 流量进行去匿名化的项目。

Reward - 一个暗中渗透 P2P 网络的项目，就像 BT 网络一样。

Mentor - 一个监控和搜索俄罗斯公司服务器上的电子邮件通信的项目。

Hope - 一个调查俄罗斯互联网拓扑及其与其他国家网络连接的项目。

Tax-3 - 一个用于创建封闭内联网的项目，用于存储高度敏感的州级人员，法官和当地政府官员的信息，与该州的其他 IT 网络分开。

另有文件显示，还有其他较旧的项目用于研究其他网络协议，如 Jabber（即时通讯），ED2K（eDonkey）和 OpenFT（企业文件传输）。

数字革命 Twitter 账户上发布的其他文件声称，FSB 也在跟踪学生和养老金领取者。虽然大多数项目只是对现代技术的研究，但有两项似乎已经在现实世界中进行了测试。

第一个是 Nautilus-S，用于对 Tor 流量进行去匿名化。 Nautilus-S 的工作始于 2012 年，两年后，2014 年，瑞典卡尔斯塔德大学的学者发表了一篇论文，详细描述了试图解密 Tor 流量的出口节点的技术进展。研究人员确定了 25 个恶意服务器，其中 18 个位于俄罗斯，并运行 Tor 版本 0.2.2.37，与泄漏文件中详述的相同。

第二个项目是 Hope，它分析了俄罗斯互联网部分的结构和构成。今年早些时候，俄罗斯进行了断网测试，在此期间，俄罗斯将其国家网络与其他互联网断开。被黑客入侵的 SyTech 公司自黑客入侵以来一直关闭其网站并拒绝媒体采访。（来源：cnbeta）

➢ 智联招聘员工参与倒卖个人信息，16 万个人简历被出售

2019 年 7 月 11 日，从北京市朝阳区人民法院获悉，一起“智联招聘”员工参与倒卖公民个人信息的案件在北京市朝阳法院第二次开庭审理。无业人员郑某为了获得公民简历信息，伪造假的企业营业执照并提供给北京网聘咨询有限公司上海分公司（简称“智联招聘”）工作人员卢某和王某，获得企业会员账号，获取大量公民简历，然后在淘宝上销售。该案涉及公民个人信息达 16 万余份。

记者了解到，被告人卢某和王某在案发前是“智联招聘”的员工，被告人郑某是一家淘宝店店主，专门在网上卖个人信息。

一条简历被卖多少钱

记者获悉，今年 5 月 6 日，朝阳区人民法院对案件进行了第一次开庭审理。1982 年出

生的郑某曾在淘宝开店卖日用品，从 2016 年开始转而买卖个人信息。在庭审中，郑某称，之前和“智联招聘”员工卢某和王某并不认识，而是认识解某，从解某处购买简历。

据了解，郑某从解某处购买了十余万份“智联招聘”的个人信息：“一份是 2.5-5 元，看下载量，偏远地区的简历便宜点，一线城市的贵些，全国区域的就更贵些。”解某的个人简历是从黄某从“智联招聘”偷来的。公诉机关指控，被告人黄某 2016 年 10 月至 2018 年 6 月间，非法进入“智联招聘”账号内，盗取个人简历信息出售给解某，违法所得 20 余万元。

解某在庭审中称，一份简历，区域的 2 元，一线城市 3.5 元，全国的 4 元。他加价五毛到一块卖给郑某。几经转手，解某将这些非法获取的个人简历信息出售给郑某，违法所得 60 余万元，而郑某通过支付宝支付钱款。

除了在解某处购买的简历，郑某还从“智联招聘”员工卢某和王某处购买了大量简历进行出售。这些个人简历信息都流向了哪里？一份能卖多少钱？记者从法院获悉，郑某在庭审中称，一份 4.5 元的简历，他加价 1 元到 1.5 元在淘宝上销售。最终，一份简历的出售价格为 5-6 元左右不等。

“智联招聘”员工协助造假出售简历

2018 年，郑某结识了在“智联招聘”工作的卢某和王某，开始从二人处购买简历。“他们有便宜的套餐，一份简历 4.5 元，一个账号 2800 份简历”郑某称。

面对公诉人的提问，郑某说了下面一段话：卢 XX 在“智联招聘”上班，是销售，他的信息会更靠谱，18 年初，他说他们有便宜的套餐，一份简历 4.5 元，一个账号 2800 份简历，但这个套餐需要企业客户提供营业执照，但我说没有营业执照，他说他认识 PS 的可以做假的，我买了 100 多个账号，卢 XX 和王 X 性质是一样的，都是“智联招聘”的销售。我在王

X 那买了 20-30 个账号。我在他俩这买的账号都是 2800 份简历一个，4.5 元一份。我给他们钱都是微信、支付宝。

按照“智联招聘”的正常信息销售流程，企业需要与“智联招聘”签订正式合同，待审批生效后再以企业账号的形式获得信息。卢某在庭审中称，郑某自称是猎头公司的，需要大量简历。于是卢某通过公司内部获取了超过 60 个企业名称，还协助郑某用 PS 伪造虚假的企业营业执照蒙混过关。郑某将钱款转至卢某的个人微信或支付宝账户，再由卢某转至公司的银行账户。

当公诉人当庭询问其做法是否符合“智联招聘”制度要求时，卢某称“领导跟我说客户给钱就行”。但他同时称自己并未从中获益。而另一位“智联招聘”的销售员王某则称，其在一开始并不知道郑某营业执照的假的，“我到后来才知道是他 PS 的”。面对公诉人“你提供企业名称，郑某就提供营业执照”是否符合常理的疑问，王某称其未考虑太多。 记者了解到，经过 5 月 6 日和 7 月 5 日两次开庭，此案未当庭宣判。

倒卖公民个人信息案件频发

记者了解到，“智联招聘”并不是第一次出现“员工参与倒卖个人简历”的案件。公开资料显示，2016 年 6 月 22 日，“智联招聘”向公安机关报案称，公司发现员工申某私下出售几十万条网站的个人简历，内容包括姓名、身份证号、住址、电话、受教育程度、工作单位、薪资收入等个人信息。该公司负责人说，按照公司的正常流程，销售人员去找有招聘需求的公司，双方签署《服务合同》，对方缴纳服务费用后，公司会提供网站简历库下载的用

户名和初始密码給对方，对方在已开通的权限内对简历库的个人简历进行下载。报案的工作人员说，公司每份简历对外的市场报价是 50 元，但申某对外的兜售价格为 2 元一份。

2017 年 6 月 2 日，申某因涉嫌非法获取公民信息罪，在朝阳法院出庭受审。经审理，法院认定其行为构成非法获取公民信息罪，判处申某有期徒刑三年六个月。

记者从中国裁判文书网公开的生效文书中看到，判决书中认定的被告人销售或购买的个人信息数量均十分可观，每次交易达上万条数据的情况十分常见。

2018 年 10 月 29 日，湖北省十堰市中级人民法院对一起倒卖公民信息案件进行宣判，被告人唐某利用工作便利，在其单位办公室内盗取全国人口信息库和全国机动车、驾驶人资源信息库，非法获取公民的个人户籍、车辆信息约 11300 余条，并将以上信息转卖，收款达十万余元。唐某还指使女友涂某帮其操作微信联系上、下线，让涂某购买公民在移动公司登记的手机号码信息约 11700 余条，并将信息倒卖，获利约 4 万余元。

2018 年 11 月 30 日，安徽省淮北市中级人民法院公布的一份判决书显示，被告人王某与他人一起在互联网上通过 QQ、微信等方式大量倒卖公民个人信息非法获利。经查，王某销售的公民个人信息（包括姓名、电话、地址等信息）累计达 5 万余条。

记者了解到，此前“两高”发布的《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》中明确规定，对于公民的行踪轨迹信息、通信内容、征信信息、财产信息，只要非法获取、出售或者提供 50 条以上，即构成“情节严重”。而对于住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息，标准则是 500 条以上。对于其他公民个人信息，标准为 5000 条以上。（来源：中国消费者报）

➢ 上海公安破获假冒“上海招考热线” 网站非法获取公民信息案

2019 年 7 月 19 日，随着“净网 2019”专项行动的深入开展，上海公安机关加大对侵犯公民个人信息等网上违法犯罪的打击力度。2019 年 7 月 8 日，上海市公安局破获一起假冒“上海招考热线”网站非法获取公民信息案，抓获犯罪嫌疑人徐某某。同时，上海市网信办依法关闭假冒“上海招考热线”网站和微信公众号。

今年 7 月，公安机关在工作中发现，假冒“上海招考热线”网站（域名：021xueli.com)和微信公众号（微信号 shzkrx）以上海市教育考试院官网上海招考热线的名称及仿冒 LOGO，盗用官网的各项招考信息，并涉嫌通过报名页面骗取考生个人信息。对

此，市公安局网安总队会同徐汇公安分局立即展开案件调查。

自该假冒网站搭建以来，犯罪嫌疑人徐某某通过该假冒网站吸引考生填写报名信息，非法获取考生信息达一万余条，并将上述数据以共享的方式传递。至案发，徐某某共非法获利十余万元。

到案后，徐某某对于通过假冒网站非法获取公民信息并牟利的罪行供认不讳。日前，犯罪嫌疑人徐某某因涉嫌侵犯公民个人信息罪，被徐汇警方依法刑事拘留。案件仍在进一步审理中。

警方提示：一是非法获取、提供公民个人信息情节严重的涉嫌犯罪。本案中，犯罪嫌疑人徐某某非法获取万余条公民个人信息后向他人提供，属情节严重，已涉嫌侵犯公民个人信息罪。在此提醒广大网民，根据《中华人民共和国刑法》第二百五十三条之一的相关规定，任何个人或单位，违反国家有关规定，向他人出售或者提供公民个人信息，以及窃取或者以其他方法非法获取公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。**二是切勿因非法利润铤而走险自毁前程。**本案中，犯罪嫌疑人徐某某近日即将与女友登记结婚，

并且已预付婚房定金正筹备贷款，崭新的人生即将开始，却因违法犯罪行为锒铛入狱，人生随之改变，悔之晚矣。在此提醒广大网民，应学法、知法、懂法、守法，增强法制意识，提高法制观念，切勿因违法犯罪行为自毁前程。（来源：警民直通车上海）